Campos Ferreira
Sá Carneiro
& Associados

FLASH

CORPORATE AND COMMERCIAL

September 2012

CHANGES TO THE LAW ON DATA PROTECTION AND TELECOMMUNICATIONS PRIVACY

1. OPENING REMARKS

Law no. 46/2012 was published in the Official Journal ("*Diário da República*") on August 29 2012. This law transposes Directive no. 2009/136/EC of the European Parliament and of the Council of 12 June ("Cookies Directive") into domestic law, introducing a first amendment to Law no. 41/2004 of 18 August, regarding the treatment of personal data and the protection of privacy in the electronic communications sector, as well as a second amendment to Decree-Law no. 7/2004 of 7 January, concerning information society services and e-commerce.

The amendments introduced by Law no. 46/2012 to the abovesaid legislation have entered into force on 30 August 2012.

In this Flash, the most significant changes brought about by Law no. 46/2012 are highlighted and briefly explained.

2. MAIN CHANGES TO LAW NO. 41/2004 OF 18 AUGUST

2.1 Definitions

Law no. 46/2012 introduces some new definitions, such as "electronic mail" (meaning "*any text, voice, sound or image message sent over a public communications network which can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient*") and "personal data breach" (with the meaning of "*a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed in connection with the provision of publicly available electronic communications services*"). The definition of "location data" was also amended to include data processed within the context of electronic communication services.

It should be noted that the definition of "electronic mail" comprises a lot more than the ordinary concept of "e-mail", reaching out to include SMS, MMS and other similar forms of communication.

2.2 Requests of access to personal data

In accordance with article 1(5) of Law no. 41/2004, as amended by Law no. 46/2012, companies rendering publicly available electronic communication services are now under the obligation to establish internal procedures allowing the processing of requests of access to users' personal data issued by competent judicial authorities in connection with issues of safeguard of public safety, defence, national security (*i.e.* State security) and the prevention, investigation, detection and prosecution of criminal offences, in accordance with the relevant legislation.

2.3 Data processing safety

The new wording in article 3 of Law no. 41/2004 imposes certain duties on companies providing communication services, namely the adoption of appropriate technical and organisational measures (taking into account the existing risks, the cost of their implementation and the state of the art of the relevant technology) in order to ensure the safety of services regarding network security. These obligations shall be fulfilled in cooperation with the provider of the public communications network, remaining the latter bound to satisfy all requests made by communication service providers deemed necessary for fulfilling their duties.

Still concerning safety measures in data processing, ICP –ANACOM is entrusted with powers to issue recommendations on best practices, to carry out inspections (directly or indirectly), including on an extraordinary basis. In the exercise of these powers and whenever data protection issues may be at stake, ICP -ANACOM shall request CNPD's opinion on the subject.

2.4 Storage and access

Article 5(1) of Law no. 41/2004 imposes the need to ensure prior express user consent for storage of information or access to information stored in the terminal equipment of such subscriber or user.

The aforesaid consent must be based upon clear and comprehensive information provided to users or subscribers in accordance with Law no. 67/98, of 26 October (Data Protection Law), which must include a description of the purposes of the intended data processing.

Law no. 46/2012 maintains the exemption established under Law no. 41/2004 (as initially enacted), which provides a carve-out for situations in which the sole purpose of access or technical storage is the transmission of communications through an electronic communications network or in which such access or technical storage is limited to what is strictly necessary in order to provide an information society service expressly requested by the subscriber or user.

These changes to the storage and access legal framework assume particular relevance due to their applicability to cookies, often used in websites. The newly enacted legislation creates an opt-in scheme for cookies, as opposed to the former existing regime, which allowed the use of cookies and merely catered for user opt-out.

2.5 Traffic and location data

Alongside the same lines, articles 6 and 7 of Law no. 41/2004 introduce the requirement of express prior consent given by a user or subscriber for the treatment of traffic and location data. Such treatment shall be strictly limited to the necessary for carrying out the consented purpose (which, in the case of traffic data corresponds to the marketing of electronic communication services or to the provision of added value services).

2.6 Notice of personal data breach

The new wording in Law no. 41/2004 enshrines, in article 3 –A, a mechanism of notification of personal data breach which was not to be found in any of the prior legislation.

In accordance with this provision, companies providing publicly available electronic communication services must promptly notify CNPD upon the occurrence of a personal data breach.

Whenever such breach may negatively impact on the user or subscriber's personal data – *i.e.*, may be prone to foster situations of identity theft or fraud, physical damage, significant humiliation or reputational damage -, providers of publicly available electronic communication services must additionally promptly notify such breach to the users or subscribers, in order to allow them to adopt the necessary precautions.

Whenever providers of publicly available electronic communication services are able to provide evidence to CNPD of the adoption of adequate protection technical measures regarding the data concerned, namely through the encryption of such data, the information duties mentioned in the previous paragraph shall not apply (article 3 – A(5)).

The notice served to users or subscribers shall contain ***i)*** a depiction of the nature of the personal data breach, ***ii)*** information on points of contact where further information may be provided, and also ***iii)*** recommendations regarding measures that can be adopted in order to curb the impact of such breach. The notice to CNPD shall, in turn, and besides the abovementioned elements, state ***iv)*** the consequences of the personal data breach and ***v)*** the proposed or adopted measures.

Providers of electronic communication services made available to the public must create and maintain a record of personal data breach situations, containing mention to their facts, effects and adopted remedies.

In our view, these provisions will not only facilitate compliance checks by the CNPD in the realm of personal data protection, but also foster the development and consolidation of best practices among companies in the management of such situations.

2.7 Unsolicited communications

Article 13 – A, newly introduced by Law no. 41/2004 imposes the requirement of prior express consent by users or subscribers for the sending of unsolicited communication for marketing purposes. This provision mentions some means of conveying such communications, which include "*automated dial and communication mechanisms not depending upon human intervention (automatic dial devices), facsimile or electronic mail*", including SMS, EMS, MMS and similar.

An exception is provided in the law for direct marketing carried out by suppliers of products or services whenever they have obtained their clients' contacts in the course of the sale of goods or the provision of services. In that case, and as long as clients are allowed to decline, easily and free of charge, the use of such contacts (both upon their collection and upon the receipt of each message), the supplier may send direct marketing communications relating to its own products or services.

Unsolicited communications for direct marketing purposes are also allowed in relation to subscribers that are legal persons, until they decline to receive such communications and request to be included in a list to be created for that purpose, maintained and updated by the entities sending such communications (in accordance with article 13 -B).

Under article 13 – A (4), sending electronic mail messages for direct marketing purposes is also forbidden whenever ***i)*** the identity of the sender is somehow concealed or omitted; ***ii)*** no valid contact that may be used to decline the reception of any further communications is provided; or iii) that encourages addressees to visit websites not compliant with the information requirements set forth in article 21 of Decree-Law no. 7/2004.

This set of provisions strikes us as particularly relevant for the analysis of situations of spam messaging, shedding light on the difference among legitimate and abusive practices regarding unsolicited communication for direct marketing purposes.

Last but not least, all providers of publicly available electronic communication services are now conferred right of action against persons in breach of the provisions mentioned in the previous paragraph, with a view to protecting their own interests and those of their clients.

2.8 CNPD and ICP-ANACOM's powers

CNPD and ICP-ANACOM's powers in connection with Law no. 41/2004 have been broadened and enhanced; currently, they also comprise rulemaking powers, as well as responsibilities of establishing and disseminating best practices and other relevant information.

Additionally, CNPD and ICP-ANACOM have also been entrusted the task of, in coordination with the European Commission, adopting measures to ensure effective cross-border cooperation in the enforcement of Law no. 41/2004, as amended.

On the one hand, under the newly adopted article 13 - E of Law no. 41/2004, entities subject to obligations under the aforesaid legislation must provide, upon ICP –ANACOM and CNPD's request, all relevant information relating to their activity. On the other hand, all information requests made by ICP –ANACOM and CNPD must be duly grounded, proportionate and adequate to the purpose they serve. If the requested information is of confidential nature, the relevant entities must identify the confidential elements and provide a reasoned explanation for refraining from disclosing them, and must as well, to the extent possible, provide ICP –ANACOM and CNPD with a non-confidential copy of any documents where that information may be found.

2.9 Sanctioning regime

In what concerns sanctioning provisions, Law no. 46/2012 establishes the minimum and maximum amounts of the fines applicable to legal persons.

Moreover, the wording of several provisions, already enshrined in the original version of Law no. 41/2004, is clarified.

Additionally, a sanctioning regime for breach of the new provisions on personal data breach and unsolicited communications is created.

The amendments introduced to Law no. 41/2004 by Law no. 46/2012 also determine the eventual application to the person in breach of a penalty for failure to comply with ICP-ANACOM and CNPD's decisions (article 15 - C). The aforesaid penalty, whose daily amount may range from € 500 to € 100 000, must be determined in a reasonable and proportionate manner, taking into account the economic situation of the person to which it is applied (namely its turnover on the previous year) and the negative impact of such breach on the market and among users.

In accordance with article 15 - A, ancillary sanctions may also be applied. These ancillary sanctions include disgorgement in favour of the State of any profits obtained as well as of any objects, equipments and illegal devices. Breach of the obligations imposed upon application of an ancillary sanction amount to serious criminal contempt of court.

3. MAIN CHANGES TO LAW NO. 7/2004 OF 7 JANUARY

Law no. 46/2012 has clarified the rules applicable to the adoption of measures against information society service providers. In particular, the new legislation has replaced the former concept of "restrictive action" ("*providências restritivas*") with the broader and more comprehensive concept of "restrictive measures" ("*medidas restritivas*").
Additionally, pursuant to the abovesaid changes to Law no. 41/2004, and in accordance with the newly enacted provisions, Law no. 46/2012 revoked certain provisions of Law no. 7/2004 relating to unsolicited communications (for instance, article 22 and article 37(1)(b)).

4. CLOSING REMARKS

The amendments introduced by Law no. 46/2012 pass on to the national legal framework the European Union policy concern with respect for personal data protection and for privacy of electronic communication users.
The entry into force of Law no. 46/2012, immediately on the day after its publication, calls for swift technical implementation of the proposed solutions, which were, nonetheless, already anticipated in the text of the so-called "Cookies Directive".
It should be borne in mind that the obligations arising from the new regime are applicable not only to companies rendering publicly available electronic communication services, but also to any other companies or persons employing electronic communications for promoting their own services or products, for instance through websites or marketing campaigns carried out using electronic means.

Lisbon, 10 September 2012