DATA PROTECTION LAWS OF THE WORLD

Portugal

DLA PIPER

PORTUGAL

Last modified 26 January 2017

LAW

Portuguese Data Protection Law – Law n°. 67/98, of October 26th – was enacted pursuant to Directive 95/46/EC.

DEFINITIONS

Definition of personal data

The Portuguese Data Protection Law defines 'personal data' as any given information, in any format, including sound and image, related to a specific or an identifiable natural person ('data subject') An identifiable person is one who can be identified, directly or indirectly, namely by reference to a specific number or to one or more elements concerning his/her physical, physiological, mental, economic, cultural or social identity.

Definition of sensitive personal data

Article 7 of the Data Protection Law defines 'sensitive personal data' as any personal data revealing one's philosophical or political beliefs, political affiliations or trade union membership, religion, private life and racial or ethnic origin and also data concerning health or sex life, including genetic data.

NATIONAL DATA PROTECTION AUTHORITY

Comissão Nacional de Protecção de Dados
*('*National Commission for the Protection of Data' also known as 'CNPD').

Rua de São Bento n°. 148, 3°
1200-821 Lisbon

T +351 21 392 84 00
F +351 21 397 68 32

geral@cnpd.pt
www.cnpd.pt

REGISTRATION

Data controllers who process personal data shall notify the Data Protection Authority ('CNPD'), unless an exemption applies. For certain categories of data (sensitive data when permitted, data regarding illicit activities or criminal and administrative offenses or credit and solvability data) and certain specific processing, prior authorisation from CNPD is required. Any variations or changes to the processing of personal data will determine the amendment of the registration.

As for the filing requirements, CNPD has an official form that must be submitted in Portuguese with the following information:

- identity of the controller and its representative
- the purposes of the processing
- third party entity responsible for the processing (data processor) if applicable
- categories of entities to which the personal data is communicated their identification and the purposes of communication if applicable
- all the personal data that will be collected in each register; it is also necessary to indicate if sensitive data is to be collected as well as data concerning the suspicion of illegal activities, criminal and/or administrative offences, as well as data regarding credit and solvability
- grounds of legitimacy of the collection and a brief description of the data collection method used
- the retention period: the way of exercising the right of access and rectification
- combination of personal data if applicable
- means and methods available for updating the data
- any transfers of data to third countries, listing the entities, the personal data transferred, the reasons of transfer and respective grounds and the measures adopted in each transfer; and
- the security and logical security measures implemented.

DATA PROTECTION OFFICERS

There is no legal requirement in Portugal for organisations to appoint a data protection officer.

COLLECTION & PROCESSING

Personal data may only be processed if the data subject has given his/her unambiguous consent or if processing is deemed necessary:

- for the execution of an agreement(s) where the data subject is party or in previous diligences for the conclusion of an agreement at the request of the data subject
- for the compliance with a legal obligation to which the controller is subject
- to protect the vital interests of the data subject if the latter is physically or legally unable of giving his/her consent
- for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data is disclosed, or
- for pursuing the legitimate interests of the controller or the third party to whom the data are disclosed, except where such interests should be overridden by the interests for fundamental rights, freedoms and guarantees of the data subject.

Moreover, the data controller must provide the data subject with all the relevant processing information, which includes the identity of the data controller, the purposes of processing, the recipients or categories of personal data and the means made available to the data subject to access, amend and delete its data.

TRANSFER

For the data transfers performed within the EU/EEA countries, it is only required to notify the CNPD and, in principle, data

processing may commence immediately thereafter.

Transfers to non EU/EEA countries can only take place if the recipient country ensures an adequate level of protection. In any case it is mandatory to start an authorisation procedure with the CNPD and data processing can only commence once the authorisation is issued.

Exceptionally, transfers performed under specific circumstances, notably according to Standard Model Clauses or to Privacy Shielf Framework holders are possible. In such cases, data processing can be done, in principle, immediately after filling with CNPD.*

CNPD issued on 10 November 2015 specific guidelines on IntraGroup Agreements (IGA) involving transfers of personal data to non EU/EEA countries.

CNPD considers that such transfers depend on prior authorisation from CNPD for the purposes of assessing if IGA's contain sufficient guarantees that the personal data transferred continues to benefit from the same level of protection as in the EU/EEA countries.

However, when such agreements follow EU model clauses, although such model clauses are designed for bilateral relationships, CNPD understands that there are reasons to authorise such transfers more quickly as long as the data controller declares that IGA is identical and that is in accordance with EU model clauses. Therefore, in the event that EU model clauses are respected within the scope of IGA, CNPD considers that the data controller, based on its declaration, has ensured the required level of protection (without prejudice to the possibility of CNPD verifying compliance with the Data Protection Law requirements and requesting a copy of the agreement.

SECURITY

The controller must implement adequate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. Specific security measures are imposed regarding sensitive personal data.

The adequacy of such measures is assessed considering whether the measures are state of the art, the costs of implementing the measures, the nature of the data and the purpose of processing.

BREACH NOTIFICATION

Law 41/2004, of 18 August on the protection and processing of personal data in e-communications as amended by Law no. 46/2012, of 29 August, which transposed Directive 2009/136/EC, establishes that companies that make electronic communications services accessible to the public shall, without undue delay, notify the CNPD of a personal data breach. When the personal data breach may affect negatively the subscriber's or user's personal data, companies providing electronic communications services to the public should also, without undue delay, notify the breach to the subscriber or user so that they can take the necessary precautions.

For these purposes, a negative effect to the personal data of privacy exists when the breach may result namely in theft or identity fraud, physical harm, significant humiliation or damage to reputation.

Regardless, if a person/entity is affected by the breach of the Data Protection Law, he/she is entitled to file a claim to the CNPD and/or file a civil lawsuit to seek compensation for damages.

ENFORCEMENT

In Portugal, CNPD is responsible for the enforcement of the Data Protection Law.

The failure to comply with data protections and privacy legal requirements and formalities may result in criminal, civil and administrative liability. Depending on the specific circumstances, crimes may be punished with imprisonment up to 2 (two) years

or fine up to 240 days and administraive offences may be punished with fine up to EUR 29,927.88 (additional penalties may be imposed).

Among other crimes, article 43 determines that any person who intentionally:

- fails to notify or seek CNPD's authorisation for data processing
- provides false information in the notification or applications for authorisation for the processing of personal data
- misappropriates or uses personal data in a incompatible manner with the purpose of the collection or with the legalisation instrument
- promotes or carries out an illegal combination of personal data
- fails to comply with the obligations provided for in the Data Protection Law or in other data protection legislation when the time limit fixed by the CNPD for complying with them has expired, and
- continues to allow access to open data transmission networks to controllers who fail to comply with the provisions of this Act after notification by the CNPD not to do so, shall be subject to a penalty up to one year's imprisonment or a fine of equivalent to 120 days.

ELECTRONIC MARKETING

The Law no. 41/2004, of 18 August on the protection and processing of personal data in e communications (as amended was recently by Law no. 46/2012, of 29 August, which transposed the 2009/136/EC Directive), determines that relation to individuals, the sending of unrequested communications for direct marketing purposes is subject to express prior consent of the subscriber or user (that is, the 'opt in' rule applies). This includes the use of automated calling and communication that do not rely on human intervention (automatic call devices), facsimile or electronic mail, including SMS, EMS, MMS and other similar applications.

This does not apply to legal entities and accordingly unrequested direct marketing communications are allowed. Nevertheless, the 'opt out' rule applies and legal entities may refuse future communications and enroll in the non-subscribers list.

This does not prevent the supplier of a product or service that has obtained its customers' data and contacts, under the lawful terms of the Data Protection Law and in connection with the sale of a product or service, to use such data for direct marketing of its own products or services similar to those transacted, provided it ensures the customers concerned, clearly and explicitly, are given the opportunity to object to the use of such data, free of charge and in an easy manner:

- at the time of the respective collection, and
- on the occasion of each message in case the customer has not initially refused such use.

The sending of electronic mail for purposes of direct marketing disguising or concealing the identity of the entity on whose behalf such communication is made, as well as the non-indication of valid means of contact to which the recipient may send a request to stop these communications or the encouragement of recipients to visit websites that violate these provisions, is strictly forbidden. The violation of these rules consists on an administrative offence, punishable with fines ranging from Eur 5,000 to Eur 5,000,000 to legal entities.

ONLINE PRIVACY

Cookie compliance

The amended Law no. 41/2004, of 18 August (as amended by Law no. 46/2012, of 29 August which transposed the 2009/136/EC Directive) determines that the storing of information and the possibility to access information stored in a subscriber/ user's

terminal is only allowed:

- if consent is based on the condition the subscriber/user has provided his or her previous consent, and
- which must be based on clear and comprehensive information, namely about the purposes of the processing.

This does not prevent technical storage or access:

- for the sole purpose of carrying out the transmission of a communication over an e-communication network, or
- if strictly necessary in order for the provider of an information society service to provide a service expressly requested by the subscriber/user.

The local regulatory Authority (CNPD) has not yet issued specific guidelines regarding the definition of 'consent', namely if implied consent suffices and if the continuous use of a website results in consent. In view of Portuguese practice and the restrictive approach taken by the DPA, we are of the opinion that implied consent shall not be enough and continuous use of a website shall only be regarded as consent provided clear and evident information is given. The use of a confirmation procedure is advisable.

Traffic Data

Traffic data must be eliminated or made anonymous when no longer needed for the transmission of the communication. Prior express consent is required and may be removed at any time. It can only be done to the extent required and the time necessary for marketing electronic communications services or the provision of value added services.

Processing of traffic data is admissible when required for billing and payment of interconnections and only until the end of the period during which the bill may lawfully be challenged or payment pursued.

Complete and accurate information on the type of data being processed must be provided, as well as the purposes and duration of the processing and the possibility of disclosure to third parties for the provision of value added services. Processing should be limited to workers and employees in charge of billing or traffic management, customer inquiries, fraud detection, marketing of electronic communications services accessible to the public, or the provision of value added services, restricting to that necessary for the purposes of such activities.

Location Data

Processing of this data is allowed only if they are made anonymous or to the extent and for the duration necessary for the provision of value added services, provided it has obtained prior express consent. Prior information must also be provided.

Companies must ensure there is an option, using simple means and free of charge:

- to withdraw consent at any time, or
- temporarily refuse the processing of such data for each connection to the network or for each transmission of a communication.

Non-compliance with 'Opt in' rules consists of an administrative offence, punishable with fines ranging from EUR 5,000 to EUR 5,000,000.

KEY CONTACTS

ABBC
www.abbc.pt/

Joao Costa Quinta
Partner
T 00351 21.3583620
j.quinta@abbc.pt

Margarida Leitão Nogueira
Associate
T 00351 21.3583620
m.nogueira@abbc.pt

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organisation's level of data protection maturity.