COELHO RIBEIRO E ASSOCIADOS
SOCIEDADE CIVIL DE ADVOGADOS

GDPR Draft Bill in Portugal

CRA – Coelho Ribeiro e Associados, SCARL
Mónica Oliveira Costa

Portugal
April 2018

On March 26 the Portuguese Parliament received the Portuguese Government Draft Bill that will ensure the implementation of the GDPR and its derogations in Portugal for assessment, discussion and approval no later than 25 May of 2018.

This is the first version which does not mean it will be the final version that the Parliament will approve. Hopefully, during the assessment and discussion of the Draft Bill in the Parliament, it will be amended in order to improve and eliminate some inconsistencies that, in our modest humble opinion, will create serious interpretation issues and serious adverse consequences for all stakeholders.

Nevertheless, it is worth to look through the Draft Bill and highlight its key concepts:

1. Scope

The Draft Bill will apply also to the processing of personal data of Portuguese data subjects living abroad and whose data are registered in the consular services.

The Draft Bill does not apply to personal data files created and maintained by the Portuguese Republic's Information System, which are ruled by specific laws.

2. Supervisory Authority

The current Data Protection Authority (Comissão Nacional de Proteção de Dados – CNPD) will be the Supervisory Authority. The current CNPD's composition and rules of procedure will be kept but its competencies are adapted to be in line with the assignments and powers foreseen in the GDPR.

It is expressly foreseen that the CNPD's members and any person mandated by the CNPD shall be bound by secrecy, which includes trade secrets to which they may have access while performing their duties.

3. DPO

The DPO is not required to have a specific professional certification and in addition to articles 37.º to 39.º of the GDPR, the DPO shall have the following tasks:

a) Ensure that periodic and unplanned audits are carried out;
b) Awareness of the users to the importance of timely detection of security incidents and the need to inform the security officer immediately whenever malicious code is detected;
c) Ensure data subjects relations regarding matters covered by the RGPD and national data protection legislation.

4. Accreditation and certification

The Portuguese Institute for Accreditation (IPAC) is the entity that will be responsible for the accreditation and certification in data protection, including seals and marks.

5. Special provisions

5.1. Minors

Child's consent in relation to information society services is lawful where the child is at least 13 years old. Below this age, consent must be given by the holder of parental responsibility or guardian, preferably through secure means of authentication.

5.2. Deceased persons

Deceased persons' personal data shall benefit from the GDPR and national legislation on data protection when such data falls in the special categories of personal data (article 9 of the GDPR). The access, rectification and erasure rights shall be exercised by his/her heirs except if a specific person was designated for that by the deceased person .

5.3. Portability and interoperability

The portability right only applies to personal data provided by their data subjects and, whenever feasible, it shall be ensured through open format

5.4. CCTV

Without prejudice of specific national legislation (such as for public security purposes) CCTV for protection of people and assets purposes shall comply with the requirements of national legislation (Law 34/2013) and the cameras or other means of image and sound capture shall not be over:

a) Public roads or neighbouring properties, except the strictly necessary to cover access to the property;
b) Zones of typing codes of ATMs or other ATM payment terminals;
c) Areas reserved for customers or users where privacy must be respected, namely sanitary facilities, waiting and dressing rooms;
d) Areas reserved for workers, namely locker rooms and sanitary facilities.

5.5. Duty of secrecy

The information and access rights foreseen in articles 13 to 15 of the GDPR shall not be exercised when the law requires the controller or the processor a confidentiality or secrecy duty that is enforceable against the data subject.

5.6. Data retention periods

Personal data shall be retained for the periods legally foreseen or in its absence for no longer than is necessary for the purposes for which they were processed.

Considering the nature and the purpose of the data processing (such as for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes) in which it is not possible to determine in advance the period of time for which the data will be required, it is lawful to retain the data.

In case the personal data is required to allow the controller or the processor to demonstrate compliance with obligations, the data can be retained as long as the limitation period does not expire.

When the data is no longer necessary for the purpose for which they were processed the controller shall destroy the data or anonymise them.

In case the retention period is legally foreseen, the erasure right shall only apply thereafter.

6. Provisions relating to specific processing situations

Among several provisions relating to specific processing situations (such as, freedom of expression and information, publication in official journal, access to administrative documents and publication of data within public procurement) we underline the following:

6.1. Context of employment

The controller (employer) shall process personal data of their employees for the purposes and under the terms and conditions foreseen in the Portuguese Labour Code, complementary legislation or in sectoral regimes, which includes the processing carried out by a processor or a certified accountant on behalf of the controller (employer) for human resources management purposes provided that such processing is governed by a service agreement and subject to confidentiality guarantees.

Unless the law provides otherwise, employee's consent is not a legitimate ground if (i) the employee may obtain a legal or economic advantage from the processing or (ii) the processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

The images recorded or other data recorded through CCTV or other technological means of remote surveillance shall only be used within criminal and disciplinary proceedings.

Employees' biometric data shall only be lawful for access and/or attendance control purposes.

Transfers of employees' data within companies that are in a Parent-Subsidiary or Group relationship or with common organisational structures are only lawful in case of temporary assignment and provided it is required, proportional and adequate for the purposes. Transfers of employees' data are also allowed in case of posting of employees to another Country.

Expectantly, the wording of the Draft Bill, at least as far as processing in the context of employment is concerned, will be amended and/or clarified. In particular, regarding consent and, above all, data transfers. In fact, this wording is not understandable nor reasonable and ultimately do not align, at all, with the GDPR's principles, ideals and purposes (e.g. BCRs which, finally, will be a legitimate ground for international transfers) nor does it safeguard the data subjects (employees) interests and rights, quite the contrary.

6.2. Special categories of personal data

Processing of special categories of personal data as foreseen in h) and i) of number 2 of article 9 of the GDPR must be carry out by a professional subject to obligation secrecy or by another person also subject to an obligation of secrecy and it shall be ensured that adequate security measures are implemented.

All controller's and processor's members, employees, service providers, DPOs as well as students, health researchers and health professionals, including those that perform follow-up, financing and inspection activities, who have access to health data are subject to obligation of secrecy.

6.3. Archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

The Draft Bill adds anonymization to the measures foreseen in number 1 of article 89 of the GDPR and expressly foresees the derogations established in number 2 and 3 of the same article 89.

Consent regarding the processing of data for scientific research purposes may cover several areas of research or be given only to certain specific fields or research projects but, in any case, it shall comply with the ethical standards recognized by the scientific community.

7. Administrative fines

The Draft Bill classifies as very serious the infringements foreseen in the GDPR that are subject to administrative fines up to 20 000 000 EUR or up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher and adds to those the infringements to the provisions relating to specific processing situations referred in 6 above.

Furthermore, it establishes minimum amounts for the fines depending of the size of the enterprises[1], as follows:

a) Between 5 000 EUR and 20 000 000 EUR or up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher, in case of a large enterprise;
b) Between 2 000 EUR and 20 000 000 EUR or up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher, in case of a small and medium-sized enterprise;
c) Between 1 000 EUR and 500 000 EUR in case of natural person.

The Draft Bill classifies as serious the infringements foreseen in the GDPR that are subject to administrative fines up to 10 000 000 EUR or up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher, and adds to those the infringements to the provisions relating to CCTV referred in 5.1 above.

Furthermore, it establishes minimum amounts for the fines depending of the size of the enterprises[2], as follows:

d) Between 2 500 EUR and 10 000 000 EUR or up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher, in case of a large enterprise;
e) Between 1 000 EUR and 10 000 000 EUR or up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher, in case of a small and medium-sized enterprise;
f) Between 500 EUR and 250 000 EUR in case of natural person.

In addition to number 2 of article 83 pf the GDPR, when deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:

[1] As defined by Commission Recommendation 2003/361/EC of 6 May.
[2] As defined by Commission Recommendation 2003/361/EC of 6 May.

a) Infringer economics status, in case of natural person, and the turnover, in case of legal person;
b) Continuing nature of the infringement;
c) Size of the enterprise, i.e., number of employees and nature of the business.

The limitation period for initiating administrative fine procedure is 3 and 2 years from the date when the infringement was committed, in case of very serious and serious infringements, respectively.

The limitation period of the administrative fines is 3 and 2 years from the decision, in case of very serious and serious infringements, respectively.

Where the administrative fine procedure results from the omission of a duty, the imposition of a fine and its payment shall not exempt the infringer from fulfilling it, should this still be possible.

Public authorities and bodies will not be subject to administrative fines, which shall be reassessed after 3 years.

8. Criminal penalties

The Draft Bill essentially maintains the same types and levels of criminal penalties foreseen in the Data Protection Act that implemented Directive 95/46/EC in Portugal (Law 67/1998 of 26 October).

9. Additional penalties

In addition to the above sanctions, it may order the temporary or definitive prohibition of the processing, blocking, erasure or total or partial destruction of the data.

For fines or crimes above 100 000 EUR, the advertisement of the conviction may be determined by means of an extract containing the identification of the infringer, the elements of the infringement and the penalties applied for a period of not less than 90 days.

10. Transitional provisions

Any notifications and authorisation applications over which the CNPD has decided before the law enters in force (ideally before or not later than 25 May 2018) shall be published in the CNPD's website.

Any pending notifications and authorisation applications over which the CNPD has not decided before the law enters in force (ideally before or not later than 25 May 2018) expire on the day the law enters in force.

The controllers and processors whose data processing have been authorised under the Data Protection Act that implemented Directive 95/46/EC in Portugal (Law 67/1998 of 26 October) shall ensure compliance with the GDPR, except as far as Data Protection Impact Assessment is concerned.

If the data processing, by the time the law enters in force, relies on consent and such consent was not given in accordance with the GDPR's requirements, new consent must be obtained within 6 months counting from the date the law enters in force or, as far as contract subject to periodic renewal, at the time of the renewal, otherwise the previous consent shall lapse.

Finally, it is also worth to emphasize the Council of Ministers Resolution n.º 41/2018, published on 28 March of 2018 that establishes the minimum compulsory and recommended technical requirements applicable to the Public Administration IT systems and networks and recommended to be applied also in the State Corporate Sector. The Public Administration shall, until 29 of September of 2019, assess their IT systems and networks and implement all the minimum compulsory and recommended technical requirements. Although it does not apply to Private Sector it is a good reference that should be considered even if for many data processing operations more demanding technical measures will be required.