August 2019

Magda Cocco | mpc@vda.pt
Inês Antas de Barros | iab@vda.pt
Adriana Oliveira Mourato| aom@vda.pt

COMMUNICATIONS, DATA PROTECTION & TECHNOLOGY

PUBLICATION OF THE GDPR IMPLEMENTATION LAW IN PORTUGAL (LAW NO. 58/2019)

Over more than a year as of the application date of the General Regulation on Data Protection ("GDPR"), Law 58/2019 was published, ensuring the implementation of the GDPR in the Portuguese legal system.

Law 58/2019 revokes Law 67/98 of October 26th (the Personal Data Protection Act - "LPDP") and republishes Law 43/2004 of August 18th, which regulates the organisation and functioning of the Portuguese Data Protection Authority ("CNPD").

The main provisions of Law 58/2019 are highlighted below:

(i) **Scope and Application**: in addition to the provisions of the GDPR, this law applies to the processing of personal data carried out outside the national territory when (a) they are processed within the scope of an establishment located in national territory or (b) they affect data subjects who are in domestic territory when the activities are subject to the scope provided for in the GDPR, or (c) they affect data registered in the consular offices of national data subjects resident abroad.

(ii) **Data Protection Officer**: Law 58/2019 extends the tasks of the DPO provided for in the GDPR, further providing that the DPO shall (a) ensure periodic and unscheduled audits; (b) make users aware of the importance of the timely detection of security incidents and of the need to immediately inform the security officer; and (c) ensure relations with data subjects in matters covered by the GDPR and national data protection legislation.

(iii) **Accreditation and Certification**: the competent authority for the accreditation and certification of data protection certification bodies is IPAC, I.P.

(iv) **Children's Consent**: children's personal data may only be processed upon consent as provided for in the GDPR and concerning the direct provision of information society services, when such children have reached the age of thirteen. If the child is under thirteen years old, processing is only lawful upon consent by the child's legal representatives, preferably through secure authentication means.

(v) **Deceased data subjects**: the data protection regime is extended to the processing of personal data of deceased data subjects insofar as they concern special data categories, data concerning privacy, image or data concerning communications.

(vi) **Video Surveillance:** without prejudice to specific legal provisions requiring the use of video surveillance (in particular for public security purposes), video surveillance systems for the protection of persons and property may not cover (a) public roads, adjoining properties or other places outside the exclusive domain of the controller, except to the extent strictly necessary to cover access to the property; (b) the area for entering ATM codes or other ATM payment terminals; (c) the inside of customer or user areas where privacy must be respected, namely toilet facilities, waiting areas and fitting rooms; (d) the inside of employee areas, including meal areas, changing rooms, gyms, sanitary facilities and break areas.

(vii) **Data storage:** Law 58/2019 establishes some specific rules concerning data storage. In particular, it provides that, with respect to personal data processed for purposes of scientific or historical research as well as for statistical purposes – where it is impossible to previously determine the moment when such processing is no longer necessary - their storage is lawful, provided that adequate technical and organisational measures are adopted to guarantee the rights of the data subject, namely the information on their storage. It further provides that where data proves necessary for the performance of contractual or other obligations, such data may be retained until the respective rights become time-barred.

(viii) **Public entities:** A set of articles establishing a special regime for the processing of personal data where controllers and processors are public entities is introduced. The processing of personal data by public entities may be carried out for purposes other than those justifying data collection, provided that public interest is at stake (misuse of data). The Law further provides that, although public entities are subject to the penalty system, they may, upon substantiated application, request the CNPD to waive the application of fines for a three-year period as from the effective date of the Law.

(ix) **Labour relations:** the employee's consent is not a lawful condition for the processing of his personal data (i) if the processing results in a legal or economic advantage for the employee or (ii) if such processing is necessary for the performance of the contract. Recorded images and other personal data of workers recorded through video systems or other technological means of remote surveillance may only be used in the context of criminal proceedings and for the purpose of establishing disciplinary liability (insofar as they are used in the context of criminal proceedings). The processing of the biometric data of employees is also limited, and may only be legitimately processed for two purposes: attendance control and access control to the employer's premises.

(x) **Health data and genetic data:** access to this type of personal data shall be granted on a need to know basis. It is also provided that the processing of health and genetic data implies that the processing is carried out by a professional bound by secrecy, or by another person bound by a duty of confidentiality or secrecy, and that appropriate information security measures are guaranteed. These measures and the minimum technical security requirements inherent to the processing of health data and genetic data shall be approved by Government ordinance.

(xi) **Fines:** fines are graduated in three levels, depending on whether the company is a large, an SME or a natural person, within the maximum limits laid down in the GDPR. Fines can range from €500 (in the case of a serious administrative offence committed by a natural person) to €20,000,000 or 4% of the total annual turnover (in the case of a very serious administrative offence committed by a large company).

(xii) **Fine calculation**: the CNPD shall take into consideration, in addition to the criteria set out in the GDPR, the economic situation of the agent in the case of a natural person, or the turnover and annual balance sheet in the case of a corporate person, the continued nature of the infringement, and the size of the entity, further taking into consideration the number of employees and the nature of services provided.

(xiii) **Crimes:** Crimes concerning personal data are typified, namely, the use of data that is incompatible with the purpose of collection, unauthorized access, diversion of data, breach of secrecy and disobedience, punishable by a prison sentence of up to one year or a fine of up to 120 days, and tampering or destroying data and the insertion of false data, punishable by a prison sentence of up to two years or a fine of up to 240 days. The attempt is always punishable concerning such crimes.