SRS ADVOGADOS
NEWS LETTER
DATA PROTECTION

August | 2019

DATA PROTECTION AND AND CYBERSECURITY

LAW IMPLEMENTING THE GENERAL DATA PROTECTION REGULATION IN PORTUGAL

After a long gestation period, **Law no. 58/2019 of 8 August ("Law no. 58/2019")** implementing the General Data Protection Regulation (GDPR) was finally published. It is a long-awaited and necessary legal act.

The GDPR expressly left it to the national legislator to define certain aspects of its implementation. The new law does this but its scope is not however limited to this as it also regulates matters such as video surveillance.

It was also essential to adapt the Portuguese data protection legal framework to the GDPR and to regulate the terms according to which the National Data Protection Supervisory Authority ("CNPD") will perform its duties under the new framework.

In this regard, Law no. 58/2019 revokes the former personal data protection law, Law no. 67/98, of 26 October and amends and republishes Law no. 43/2004 of 18 August, which provides for the CNPD's powers and structure.

Amongst the matters that Law no. 58/2019 has consolidated, the following should be highlighted:

1. In the context of **labour relations**, the new law indicates the instances where the processing of workers' personal data is not subject to consent, and the use of images recorded by video surveillance systems is regulated.

2. The lawfulness of the processing of **workers' biometric data** is limited to the control of attendance and control of access to the employer's premises and the controller must ensure that only representations of the biometric data are used and that their collection process ensures that such representations are non-reversible;

3. In the processing of **health data** and **genetic data**, access to personal data is governed by the principle of necessity. In certain cases, access to health data may take place exclusively by electronic means and an obligation to notify the data subject of any access to his/her personal data has been put in place.

4. In addition, the law establishes the minimum technical safety requirements for the processing of **health** and **genetic data**, which will be adopted in the future by a statutory instrument;

5. With regard to the use of **video surveillance systems** the law introduces limits concerning the orientation and placement of cameras and prevents recordings of sound, except when the facilities in question are closed to the public or if the CNPD expressly authorises such recordings;

6. Moreover, the law clarifies that the performance of the duties of the **Data Protection Officer ("DPO")** does not require any professional certification and a duty of professional secrecy is introduced, which remains enforceable after the expiry of the DPO's mandate;

7. The law also specifies that the **DPO's functions** include (i) ensuring that audits are performed, (ii) making users aware of the importance of early detection of security incidents, and (iii) to interact with data subjects in matters relating to the protection of personal data; the designation of DPOs by public and private authorities is regulated;

8. As regards the offer of information society services, the law provides that the **age of consent** concerning the processing of personal data of **minors** is **13 years**; such consent is provided preferably by means of secure authentication;

9. Certain categories of data relating to **deceased persons** are protected under the terms of the GDPR and Law no. 58/2019; in particular, the rights of access, rectification and erasure are exercised by the person designated by the deceased for this purpose, failing which the heirs of the deceased may exercise such rights; finally, data subjects may expressly object to the exercise of the above refereed to rights after their death;

10. The law clarifies that the **right to data portability** covers only the data provided by the respective data subjects and, where possible, portability should take place in open format;

11. Specific rules for the **storage** of data are set forth; the law establishes the duty of destruction or anonymization of personal data, when the purpose of such processing ceases to exist;

12. The exercise of data subjects' **rights of information and access** to personal data is excluded when the law imposes on the controller or the processor a duty of secrecy that prevails over those rights;

13. The responsibility to **accredit the data protection certification bodies** has been granted to the Portuguese Institute of Accreditation, I.P. ("IPAC, I.P.");

14. Finally, the publication of personal data in an **official journal** and the publication of data in the context of **public procurement** procedures are specifically regulated; these matters gave rise to controversy as a result of the application of the GDPR.

Law no. 58/2019 confirms the role of **CNPD** as a supervisory authority, empowering it, in addition to the powers set forth in Article 57 of GDPR, to:

a) Advise, on a non-binding basis, on legislative and regulatory measures concerning the protection of personal data;
b) Supervise the compliance with the GDPR and other legal and regulatory instruments relating to data protection;
c) Make available a list of processing operations subject to data protection impact assessment (a list that has already been made available under CNPD Regulation no. 1/2018);
d) Develop and submit to the European Data Protection Board ("EDPB"), as provided for in the GDPR, draft criteria for the accreditation of codes of conduct, of monitoring bodies and of certification bodies; and
e) Cooperate with IPAC, I.P. in the accreditation and certification processes.

The GDPR has established particularly high **fines** for non-compliance. There are two thresholds for fines: the first is up to €10 million or 2% of the company's global annual turnover for the previous financial year, whichever is higher. The second is up to €20 million or 4% of the company's global annual turnover for the previous financial year, whichever is higher.

Law no. 58/2019 sets the **minimum amounts** of these fines, namely €500 when the offenders are natural persons, €1.000 in the case of SMEs and €2.500 when the infringement is committed by a large company[1].

As was the case before, 60% of the amount of the fines levied reverts to the State and 40% to the CNPD.

Contrary to the intention expressed in the Government's draft law, **public entities** will also be subject to **fines** for failure to comply with legal obligations, without any "grace period". However, Law no. 58/2019 provides that the same entities may submit to the CNPD a duly substantiated request for a penalty exemption for a period of three years from the entry into force of that law.

Law no. 58/2019 also establishes a set of criminal offences, with penalties of up to 4 years' imprisonment or daily fines for a maximum of 480 days. Such crimes are namely:

- Use of data in a manner incompatible with the purpose of collection;
- Undue access;
- Data deviation;
- Data vitiation or destruction;
- Entering false data;
- Breach of duty of confidentiality; and
- Disobedience.

Despite the long gestation period and the legislator's effort to receive the input of all the relevant actors of civil society, Law no. 58/2019 is silent on certain fundamental aspects, such as the need for insurance companies to process health data in certain circumstances without consent. Its interpretation and concrete application will certainly raise numerous questions in the future.

[1] The concepts of 'SME' and 'large enterprise' are those defined in the European Commission Recommendation 2003/361/CE, of 6 May 2003.