PLMJ

AUG. 19

INFORMATIVE NOTE

TECHNOLOGY AND PRIVACY

The 12 fundamental points of Portuguese law that ensure the Implementation of the General Data Protection Regulation

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the General Data Protection Regulation or GDPR) began to apply more than one year ago. Reaching this point involved a long legislative process marked by advances and setbacks, and the process culminated with the publication of Law 58/2019 of 8 August – the law that implements the GDPR into Portuguese law.

The aim of this Law is to implement certain aspects of the GDPR that were left to the discretion of the Member States. It amends Law 43/2004 of 18 August, which is the law that regulates the organisation and functioning of the National Data Protection Commission (CNPD) and the personal status of its members. The new Law also explicitly repeals Law 67/98 of 26 June (the Data Protection Law).

However, a first reading of the Law makes it clear from the outset that this is more than simply a law implementing the GDPR. In fact, the Law not only regulates the issues left open by the GDPR. It also establishes rules that go beyond what would be expected in a national law implementing a European regulation. Indeed, in the promulgation note itself, the President of the Republic recognised that *"(...) the national legislation does not (...), as the CNPD states in its opinion, include greater attention to the economy of the rules and a greater clarification of the rights and freedoms concerning the processing of personal data".*

Portugal was one of the few EU Member States that had still not updated its data protection rules to align them with the GDPR. Therefore, the publication of this law is of great importance.

As a result, we now provide a summary list and description of the 12 main changes in the new rules.

Daniel Reis
Rita de Sousa Costa
Technology Team and privacy

"In fact, the Law not only regulates the issues left open by the GDPR. It also establishes rules that go beyond what would be expected in a national law implementing a European regulation."

1. Data protection officer (articles 9 to 13)

The new Law adds to the duties enshrined in the GDPR for the data protection officer (DPO). It provides that the DPO has "to ensure that audits are carried out either periodically or on a non-programmed basis; to make users aware of the importance of timely detection of security incidents and of the need to inform the security officer immediately; and to ensure relations with the data subjects on matters covered by the GDPR and by national legislation on data protection."

The Law also enshrines two sets of rules addressed to data protection officers in public bodies and data protection officers in private bodies.

"The Law also enshrines two sets of rules addressed to data protection officers in public bodies and data protection officers in private bodies."

In the rules on data protection officers in public bodies, the Law first determines what is meant by public bodies for this purpose. It defines public bodies as the State, the autonomous regions, the local authorities and supranational entities provided for by law, the independent administrative entities and Banco de Portugal, the public institutions, the public higher education institutions, regardless of their nature, companies in the state business sector and in the regional and local business sectors, and the public associations.

Under the new rules, the same data protection officer may be assigned to various ministries or government departments, regional secretariats, local authorities or other public bodies. It is not mandatory for the role of data protection officer to be performed on an exclusive basis. However, in the case of a public body with regulatory or control powers, the data protection officer may not simultaneously act in that capacity in a body subject to the control of the regulatory body or within its "regulatory purview".

2. Accreditation, certification and codes of conduct (articles 14 and 15)

The Law determines that the authority with power to award accreditation to certification bodies in the field of data protection is the IPAC, I.P. In turn, the certification is performed by bodies accredited by the IPAC, I.P.

The processing of personal data by the direct and indirect administration of the State is subject to its own code of conduct.

3. Consent of minors (article 16), consent in employment relationships (article 28) and renewal of consent (article 61)

The age of consent for minors was fixed at 13 years of age. Therefore, the consent of children under 13 years must be given by their legal representatives.

In the context of employment relationships, the Law provides that the consent of the employees does not make the processing lawful if it results in a legal or economic advantage for the employee, or if the processing is covered by the scope of performance of the contract of employment.

Finally, the Law establishes that if the consent given prior to the entry into force of the Law meets the requirements of the GDPR, it will not be necessary to obtain new consent from the data subject.

4. Protection of the personal data of deceased persons (article 17)

The Law establishes a rule intended to protect certain personal data of deceased persons, in particular, the special categories of personal data referred to in the GDPR and data that relate to the intimacy of private life or image, or the data relating to communications. Under the Law, the rights of access, rectification and erasure are exercised by a person designated by the data subject in life, or, when this does not happen, by their heirs. However, the data subject is also allowed to determine the impossibility of exercising those rights after their death.

5. Video-surveillance (article 19)

The main rules on video-surveillance remain in force in Law 34/2013 of 16 May. However, the new Law does establish some limits on what video surveillance cameras may record. Some of these limits came (from the previous rules and) from the case law of the Court of Justice of the European Union (see, e.g., Ryneš, C-212/13). Thus, among others, the Law safeguards the rules that cameras cannot be focused on public roads, areas where codes are typed into cash machine or ATM payment terminals, the interior of areas reserved to customers or users such as bathroom facilities or changing rooms, and the interior of areas reserved to employees, such as dining areas and locker rooms, etc. The Law also provides that in educational establishments, cameras can only focus on external areas, entrances and areas such as laboratories or computer rooms.

The GDPR has abolished the prior control in force under the previous rules, through the issuance of permits by the national supervisory authorities (in the case of Portugal, the CNPD). However, the new Law does retain a remnant of these rules in establishing that video surveillance with sound recording is only permitted (whether in the period the premises subject to surveillance are open closed or) upon prior authorisation from the CNPD.

6. Period of storage of personal data (article 21)

The GDPR establishes the principle of limiting the period for which data is stored. However, under the new Law, the period for storing personal data is what is stipulated by legal or regulatory rule or, in the absence of this, whatever is necessary to achieve the purpose". In contractual matters, personal data may be stored until the end of the limitation period for the corresponding rights. When the purpose no longer exists, the data must be deleted or anonymised. However, the law establishes a rule that specifically addresses the reconstitution of contributory careers, in which case the data can be stored without a time-limit.

PL
MJ

7. Data processing by public authorities for purposes other than those for which they were collected (article 23, publication of data in an official journal (article 25) and publication of data in the context of public procurement (article 27)

The processing of data by public authorities for a purpose other than the one for which they were collected must be exceptional in nature, properly reasoned and ensure the pursuit of a public interest that could not otherwise be protected. Furthermore, the transfer of personal data between public bodies for different purposes must be subject to a protocol between them.

As regards publication in the official journal, the personal data that appears in these publications may not be altered, erased or hidden. Furthermore, the right to be forgotten is subject to stringent restrictions. These include the fact it can only be exercised in very exceptional cases and "through the de-indexation of personal data in search engines, always without eliminating it from the publication that evidences it".

Finally, with regard to data published in the context of public procurement, whenever the name is sufficient to identify the public contractor and co-contractor, no other personal data should be published.

8. Processing of personal data in employment relationships (article 28)

Besides the considerations relating to the consent given by employees in the context of the employment relationship addressed above, the Law also lays down rules on the use of means of remote surveillance and on the processing of biometric data.

"The Law also lays down rules on the use of means of remote surveillance and on the processing of biometric data."

Regarding remote surveillance, the Law establishes a set of limitations on the use of recorded images or other data recorded by means of remote surveillance. These rules are intended to align with the principles contained in the Employment Code. One of the main changes made in this respect is the provision that any images or other data recorded by means of remote surveillance may only be used in the context of criminal proceedings. Moreover, in this case, the images or data recorded by those means can also be used to establish disciplinary responsibility.

However, the processing of biometric data is only considered lawful to check attendance and check access to the employer's premises. In this case, it must be ensured that data reversibility is not possible.

9. Processing of health data and genetic data (article 29)

The Law establishes that processing personal data necessary for certain purposes must be carried out by professionals subject to a confidentiality obligation. These purposes are preventive or occupational medicine to evaluate an employee's capacity to work, medical diagnosis, the provision of health or social action care or treatment, the management of health or social action systems and services, as well as the personal data processing necessary for public interest reasons in the field of public health. The data listed above is accessed exclusively electronically, unless that is technically impossible or there is an express indication to the contrary by the data subject.

The data controller responsible for processing health data and genetic data must ensure a traceability and notification mechanism is provided. This is because the Law provides that the data subject has the right to be notified of any access made to their personal data.

Finally, the processing of health data and genetic data is subject to minimum technical security measures and requirements that will be detailed in a ministerial order.

10. Processing for public interest archive purposes, scientific or historical research purposes, or statistical purposes (Article 31(2))

There may be some derogation from the rights of data subjects for the purposes personal data processing for public interest archive purposes, scientific or historical research purposes, or statistical purposes, if their rights compromise these purposes. This is the case, in particular, of the rights of access, rectification, limitation of processing and opposition.

11. Judicial protection (article 34) and the CNPD's legal standing (article 36)

Actions brought against the CNPD are heard by the administrative courts and this includes actions relating to administrative offences.

The Law also stipulates that "the CNPD has standing to intervene in judicial proceedings involving infringements of the provisions of the GDPR and of this law". It does not contain any rule equivalent to article 22(6) of Law 67/98, concerning representation of the CNPD in court, which was done by the Public Prosecutor.

12. Sanctions

a. Administrative offences (articles 37 to 45)

The Law classifies administrative offences as "very serious" and "serious".

"Very serious" administrative offences can be punished, depending on who commits them, with the following fines:

- Large company: €5,000 to €20,000,000, or 4% of annual turnover considered on a global level, whichever is greater;
- SMEs: €2,000 to €20,000,000, or 4% of annual turnover considered on a global level, whichever is greater;
- Individuals: €1,000 to €500,000.

"Serious" administrative offences can be punished, depending on who commits them, with the following fines:

- Large company: €2,500 to €10,000,000, or 2% of annual turnover considered on a global level, whichever is greater;
- SMEs: €1,000 to €1,000,000, or 2% of annual turnover considered on a global level, whichever is greater;
- Individuals: €500 to €250,000.

When deciding the level of the fine, in addition to the criteria laid down in the GDPR, the following criteria are also applicable: "the economic situation of the agent, in case of an individual, or the turnover and the annual balance sheet, in the case of a legal entity", "the continuing character of the offence" and "the size of the entity, taking into account the number of employees and the nature of services rendered".

Another change made by the Law is that bringing administrative offence proceedings always depends on a prior warning being given by the CNPD to comply with the obligation not fulfilled or to remedy the prohibition breached within a reasonable time, except when there is intent.

In the case of "very serious" administrative offences, the possibility to bring the proceedings is time-barred three years after the commission of the offence. In the case of "serious" administrative offences, it is time-barred after two years.

Fines exceeding €100,000 are time-barred after three years and fines of £100,000 or less are time-barred after two years.

The fines apply to both private and public bodies. However, in the case of the latter, the Law provides that they may make a reasoned request to the CNPD for the fine not to be applied during the period of three years from the date of entry into force of this Law.

The rules that apply to administrative offences on a subsidiary level are contained in the General Framework for Simple Administrative offences.

b. Crimes (articles 46 to 54)

The main changes made in relation to Law 67/98 with regard to sanctions of a criminal nature are:

In relation to the crime of unauthorised access, if the access relates to personal data covered by articles 9 and 10 of the GDPR, the penalty limits are double the maximum.

The sanction for the crime of breach of the duty of secrecy was reduced from up to two years in prison or a fine of up to 240 days, to up to one year in prison or a fine of up to 120 days.

All the crimes in this Law are public crimes and this represents a change in relation to the Law 67/98, in which the crime of unauthorised access depended on a complaint being made.

As under the previous rules, an attempt is punishable.

Finally, the following additional sanctions can be imposed: prohibition on processing, blocking and total or partial erasure of data. In the case of crimes or of fines exceeding €100,000, the Law provides for the possibility to publicise the conviction on the government website *eportugal* for a period of not less than 90 days.