SEPTEMBER 2019

IMPLEMENTATION OF THE GENERAL DATA PROTECTION REGULATION IN THE PORTUGUESE LEGAL SYSTEM

Scope and Assumptions under Law no. 58/2019 of the 8th August.

Law no. 58/2019, establishing the measures and conditions for the implementation, within the national legal system, of the General Data Protection Regulation (GDPR), was recently published.

1. Scope of Application

At the time of its publishing, the GDPR gave Member States discretion to legislate on several issues. In the context of such discretion, Law no. 58/2019 aims not only at implementing the GDPR but also at regulating different matters, namely (*i*) the responsibilities of the Data Protection Officer (DPO), (*ii*) the supervision, accreditation and certification in relation to personal data matters; (*iii*) data processing for underaged people, deceased, employees, heath-related and genetic data, (i*v*) the deadline for storing personal data and (*vi*) the criminal and misdemeanour framework.

2. Responsibilities of the Data Protection Officer

Law no. 58/2019, complementing the GDPR, extends the responsibility attributed to the DPO by the regulation. As such, the DPO also becomes responsible for:

- Ensure auditing, both periodic and unscheduled;
- Raise awareness among people working for and with the -----for the significance of the timely detection of security incidents and for the immediate need to inform the security officer;
- Ensure the dealings with the data subjects in matters relating to the GDPR and to the national legislation for data protection.

Rua Alexandre Herculano, n.º 23 - 2.º
1250-008 Lisboa Portugal
T. +351 21.093.64.04 F. +351 21.093.74.07
www.paresadvogados.com
geral@paresadvogados.com

3. Supervision, Accreditation and Certification

Law no. 58/2019 has appointed the National Data Protection Commission (CNPD) as responsible for the the supervision and control not only of the GDPR but also of the law itself.

In turn, the Portuguese Institute for Accreditation (IPAC) was named as responsible for the accreditation of the certifying bodies in what refers to data protection.

4. Underaged people, deceased, employees, health-related and genetic data

Law no. 58/2019 substantiates some rules in relation to data processing of underaged people, deceased, employees and health-related and genetic data:

(i) Data of underaged people, insofar as it relates to the direct offer of services of the information society

Law no. 58/2019 establishes 13 years of age as the reference age from which the consent of the holders of parental responsibilities is no longer necessary. As such, the data processing of persons younger than 13 years of age is subject to the consent of the holder of the parental responsibilities (which should be asserted, preferably, using means of secure authentication).

(ii) Data of deceased people

Law no. 58/2019, unlike the GDPR which leaves out any protections in this regard, safeguards the processing of data of deceased people that might be considered sensitive, i.e., those that are part of the special categories of personal data[1], that are private, refer to image or communication. Now, the processing of these has to account for the rules of the GRPR.

(iii) Employees' personal data

Law no. 58/2019 confirms what the GDPR prescribes: the processing of data of the employee does not depend on its authorisation, when it is necessary for the execution of the employment contract.

Still in this context, Law no. 58/2019 also stipulates that consent also is not necessary

[1] According to article 9 of the GDPR special categories of personal data are those which 'reveal the racial or ethnic origin, political opinions, religious or philosophical beliefs, union membership as well as the processing of genetic data, biometric data in order to unequivocally identify a person, health-related data, or data pertaining to the sexual life or sexual orientation of a person.'

if the processing of personal data results in a legal or economic advantage for the employee (for instance, in respect to health or life insurance or assignment of a vehicle).

Law no. 58/2019 also clarifies some doubts raised by the former legal framework:

a) The processing of an employee's biometric data only is legitimate in order to (*i*) monitor attendance and (*ii*) monitor access to the employer's premises;
b) Data collected by the employer, through video surveillance systems or other remote surveillance technological means, can only be used for disciplinary reasons when disciplinary and criminal responsibility simultaneously result from the behaviour of the employee.

(iv) Health-related and genetic data

Law no. 58/2019 only implements what is prescribed in the GDPR, among others:
(*i*) access to health-related and genetic data shall be governed by the need to know the information and
(*ii*) the processing of health-related and genetic data should be conducted by a professional bound by professional confidentiality or by someone subject to confidentiality. In this context, necessary and adequate measures and requirements should be put in place to ensure the secure processing of data.

5. Storage of Personal Data

Law no. 58/2019, as occurs with unlike the GDPR, does not establish a specific deadline up to which personal data should/can be stored.
In this matter, the law refers to the deadline considered necessary for the pursuit of the purpose for which the personal data was collected.

It also adds that, in those cases where the controller or the processor need the personal data to demonstrate the compliance with a contractual or non-contractual obligation, the data can be stored in accordance with the legal deadlines.

6. Criminal and Misdemeanour Framework

In what refers the misdemeanour framework, Law no. 58/2019 prescribes three

distinct frameworks to be applied depending on the type of agent committing the misdemeanour:

1. Large corporation
2. Small and medium enterprise (PME) or
3. Natural person

The amount of the fine will also depend on whether the misdemeanour is classified as serious or very serious.

As such, considering the agent committing the misdemeanour and the type of misdemeanour, one of the following fines can be applied:

	Large Corporation	**PME**	**Natural Person**
Very serious misdemeanour	€ 5,000.00 to €20M or 4% of the yearly worldwide turnover	€ 2,000.00 to €2M or 4 % of the yearly worldwide turnover	€ 1,000.00 to €500,000.00
Serious misdemeanour	€ 2,500.00 to €10M or 2 % of the yearly worldwide turnover	€1,000.00 to €1M or 2 % of the yearly worldwide turnover	€500 to € 250,000.00

Concerning the potential criminal liability emerging from "personal data crimes", Law no 58/2009, envisages the following crimes and penal frameworks:

Crime	**Penalty**	
	Prisão	Fine
Use of data in any way which is inconsistent with the purpose of the collection	Up to 1 year	Up to 120 days
Diversion of data	Up to 1 year	Up to 120 days
Tampering or destruction of data	Up to 2 years	Up to 240 days
Input of false data	Up to 2 years	Up to 240 days
Breach of the duty of confidentiality	Up to 1 year	Up to 120 days
Disobedience	Up to 1 year	Up to 120 days

Rua Alexandre Herculano, n.º 23 - 2.º
1250-008 Lisboa Portugal
T. +351 21.093.64.04 F. +351 21.093.74.07
www.paresadvogados.com
geral@paresadvogados.com

* * *

PARES | Advogados is available to provide more information about the legislation on data protection.

José Maria Simão
jms@paresadvogados.com

João Fernandes Thomaz
jft@paresadvogados.com