
Intellectual Property, Media and IT

Newsletter | Portugal

3rd Quarter 2019



Contents

- > **The Portuguese Data Protection Authority declares national provisions incompatible with the General Data Protection Regulation**
- > **National legislation**
- > **Case law**
- > **Regulations, resolutions, recommendations, opinions and other**



I. The Portuguese Data Protection Authority declares national provisions incompatible with the GDPR

On September 3, 2019, the Portuguese Data Protection Authority (“CNPD”) issued resolution 2019/494, declaring several provisions of Law 58/2019, of August 8, unenforceable. Law 58/2019 ensures the execution in Portuguese territory of Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation, or “GDPR”).

The CNPD concluded that it had the power to declare these incompatible provisions unenforceable.

The CNPD highlights that its legal powers are based on the principle of supremacy of European law and the direct applicability of European regulations in national legal systems. Under the case law of the Court of Justice of the European Union (“ECJ”), all public entities, including administrative and judicial ones, must disregard national provisions that are incompatible with European law.

Unenforceable national provisions:

- **Article 2, no. 1 and 2 determines the objective and subjective scope of national jurisdiction over supervising data protection. The law established that national jurisdiction applies to data processing “carried out within the scope of an enterprise established in the national territory.”**

The CNPD considered that this provision jeopardized the application of procedural and jurisdiction distribution rules between the national supervisory entities of the Member States in cases of cross-border processing activities.

If the data processor or subcontractor has more than one establishment in the EU, article 56 of the GDPR establishes the criteria to determine the national authority responsible for directing the procedure and issuing the final decision. This one-stop-shop mechanism ensures a healthy distribution of competences between the supervisory authorities of the Member States of the EU.

The key rule is that the authority of the Member State in which the data processor’s main establishment is located is the main supervisory authority.

However, under Law 58/2019, the CNPD would have jurisdiction over the data processing that a data processor carries out in Portugal, regardless of whether its main establishment is in another Member State of the EU.



The CNPD considered these provisions incompatible with article 56 of the GDPR, as they would cause an overlap of supervisory jurisdictions between national authorities, so it declared these national provisions unenforceable.

- **Article 20, no. 1 states, “The right to information and access to personal data under articles 13 and 15 of the GDPR must not be exercised when the law imposes on the controller or processor a duty of secrecy to the data subject.”**

Regarding the indirect collection of personal data, the GDPR already imposes all the restrictions on exercising these rights. Therefore, the CNPD considers the national law redundant, and it will disregard it when supervising the GDPR’s implementation.

Regarding the direct collection of data, articles 13 and 15 of the GDPR do not impose any restrictions on exercising the right to access.

Under article 23 of the GDPR, Member States may only restrict the right to access if *“this limitation respects the essence of fundamental rights and freedoms and constitutes a necessary and proportionate measure in a democratic society.”*

As the CNPD notes, the national provision does not specify the legitimate reasons for processing data, a requirement established under article 23 of the GDPR. Consequently, the CNPD considered this provision unenforceable.

- **Article 23 allows public entities to process and transfer data for purposes other than those for which the data was originally collected, provided they issue a resolution identifying how reusing the data is in the public interest.**

Article 6, no. 4 of the GDPR allows public entities to reuse data, provided it is a *“necessary and proportionate measure in a democratic society to safeguard the objectives referred to in article 23 (1) of the GDPR.”*

However, the CNPD considered the national provision too broad to comply with these articles and the principle of purpose limitation under article 5 of the GDPR.

According to the CNPD, under the GDPR, data processors must assess each step involved in reusing data. However, it does not allow abstract provisions that fail to specify how reusing the data is in the public interest.

- **Article 28, no3 (a) states, “Unless stated otherwise, employees’ consent must not constitute a requirement for a legitimate processing of their personal data: a) if the advantage or economic benefits for the employee results from the data processing (...).”**



The CNPD considered this provision an “*inappropriate, unnecessary and excessive restriction of the fundamental right to informational self-determination and the employees’ right to control their own data.*” This is because it disregards an individual’s free will to make decisions about his or her personal data.

The CNPD considered that the provision greatly undermines the importance of employees’ consent, ignoring circumstances in which they may authorize their employers to process their data, provided it does not breach their rights or jeopardize their interests.

Penalties

- **The penalties established in national legislation under article 37, no 1 (a), (h) and (k), and no. 2 differ from those established in the GDPR.**

Subparagraph (a) provides that the intentional failure to comply with the data protection principles set out in article 5 of the GDPR will result in a penalty. However, this penalty is already established in article 83, no. 5 (a), regardless of the data controller or data processor’s intent or negligence.

Subparagraph (h) presents a similar problem, as it establishes a penalty for those who do not comply with the obligation to provide “relevant” information. However, article 83, no. 5 (b) of the GDPR does not define the nature of the information (i.e., relevant or otherwise).

Subparagraph (k) establishes a major penalty for not cooperating with the national supervisory authority for data protection. However, article 83, no. 4 (a) establishes an ordinary penalty.

Therefore, the CNPD considered these three subparagraphs incompatible with the GDPR, i.e., unenforceable.

- **The fine limits established in article 37, no. 2 and article 38, no. 2 differ from those established in article 83, nos. 4 and 5 of the GDPR. In the national provisions, the fine depends on whether the offender is a large enterprise, a small or medium-sized enterprise, or an individual.**

The CNPD highlights that article 83 of the GDPR is a legislative mandate to the national supervising authorities of each Member State, but not to national legislators. The CNPD understands that Member States cannot establish different fine limits or criteria in their national laws.

In fact, the CNPD considered that there was no room for “*consideration of the size of an enterprise, so the criteria the national legislator adopted to distinguish small and medium-sized enterprises so it could impose the highest fines on large enterprises is a breach of the GDPR.*”



The CNPD applied the same reasoning to the limitation of fines for individuals.

- **Article 39, no. 1 established three criteria that the CNPD must consider when determining the fine (in addition to those established in article 83 of the GDPR).**

The CNPD stated, *“The GDPR leaves no room for Member States to define further weighting criteria for the penalties established in article 83, no. 4 and 5.”*

The CNPD further stated that, under article 83, no. 2 (k) of the GDPR, other aggravating or mitigating factors of the infringement may be considered. However, it deemed that *“the choice of these factors is for specific cases only, decided on by the entity (administrative or judicial) applying the fine, but not by the national legislator of each Member State.”* Therefore, the CNPD found the provisions establishing additional criteria unenforceable.

- **Article 39, no. 3 states, “Except in cases of intentional misconduct, before starting an infringement procedure, the CNPD must first issue a warning to the agent, ordering him or her to stop breaching the data processing provisions within a reasonable timeframe.”**

The CNPD considered this legal obligation to issue a warning to a negligent offender to stop the unlawful conduct within a reasonable timeframe was an unauthorized limitation of the discretionary powers granted by the GDPR. Consequently, this provision was incompatible with the GDPR, i.e., unenforceable.

- **Article 61, no. 2 sought to safeguard data controllers that handle health and life insurance contracts by stipulating that consent would only be revoked once the insurance contract is terminated.**

According to the CNPD, **article 61**, no. 2 confuses two separate requirements to process data (one being consent and the other to perform a contract). The CNPD considered the performance of a contract to justify processing the data necessary to execute the contract.

Controllers are only obliged to obtain the data subject’s consent when they intend to carry out other processing operations that are not necessary for performing the contract. Therefore, they do not need to obtain the data subject’s consent to process the data necessary to perform the contact.

However, the CNPD did not take a position on whether the GDPR allows insurers to legitimately process sensitive data (e.g., health information) to perform contracts.

Therefore, it is not clear whether (or how) insurers should process essential sensitive data to offer health and life insurance products.



- **Article 62, no. 2 states, “None of the provisions on authorizations or notifications of data processing (...) will apply as of the date the GDPR enters into force.”**

The CNPD highlighted that this provision applied the GDPR retroactively (back to May 25, 2016), even though the GDPR had a two-year transition period. The CNPD considered this provision a breach of article 99, no. 2 of the GDPR.

To conclude, the CNPD’s decision to declare these national provisions unenforceable is in line with the principle of supremacy of EU law. Public authorities are obliged to rule on whether national provisions are enforceable and to recognize citizen’s rights that could otherwise be restrained by national law. This obligation applies to all administrative entities (including the CNPD) and judicial entities such as courts.

In several judgments (e.g., [Decision C-103/88 - Fratelli Constanzo](#)), the ECJ has already ruled that national public authorities must disregard national provisions when they impede the direct applicability of European regulations or when Member States fail to transpose European directives into their national legal systems.

Both European and national legal doctrine support the ECJ’s understanding.

The CNPD’s resolution does not create any legal loopholes, as it enables the GDPR to be applied directly without any impediments.

If the CNPD were to change its position and reapply any rules that it had previously declared unenforceable (e.g., should a court disagree with its interpretation of national provisions), data controllers and processors would not be jeopardized for processing data in accordance with an invalid interpretation of the GDPR.

II. National legislation

Ordinance 201-A/2019, enacted on July 1, 2019, updating the rates and foreseeing new rates arising from the acts inserted in the new Industrial Property Code, as well as revoking Ordinance 1098 enacted on September 30, 2008.

Decree-law 89/2019, enacted on July 4, 2019, modifying collective management entities, copyright and related rights.

Rectification Amendment 32/2019, enacted on July 4, 2019, rectifying Ordinance 201-A/2019 enacted on July 1, 2019, published in the Official Gazette, 1st Series, no. 123 (industrial property rights).

Decree-law 90/2019, enacted on July 5, 2019, changing the modus operandi for artistic shows and the setting up and supervision of the fixed enclosures intended for their



performance, as well as the classification of shows of an artistic nature and for public entertainment.

Law 46/2019, enacted on July 8, 2019, modifying the regime for carrying out private security and self-protection activities.

Law 55/2019, enacted on August 5, 2019, attributing new competencies to the Intellectual Property Court, changing (for the eighth time) the Legal System Organization Act, approved by Law 62/2019, enacted on August 26, 2013.

Law 58/2019, enacted on August 8, 2019, ensuring the implementation, under national law, of (EU) Regulation 2016/679 of the European Parliament and of the Council of April 27, 2016, on the protection of individuals with regard to personal data processing and the free movement of such data.

Law 59/2019, enacted on August 8, 2019, approving the rules on personal data processing to prevent, detect, investigate and prosecute criminal infringements or to implement criminal sanctions, transposing (EU) Directive 2016/680 of the European Parliament and the Council of April 27, 2016.

Ordinance 289/2019, enacted on September 5, 2019, regulating complementary aspects of the electronic invoice.

Order 7450-A/2019, enacted on August 21, 2019, determining the coming into force of Law 30/2019, enacted on April 23, 2019, which introduces restrictions to advertising aimed at the under-16 of high-energy food and drinks and those with high a content of salt, sugar, saturated fatty acids and trans fatty acids.

Ordinance 326/2019, enacted on September 23, 2019, modifying the statutes of the National Institute for Industrial Property (*Instituto Nacional da Propriedade Industrial, I. P.*), approved as an annex to Ordinance 386, enacted on November 29, 2012.

III. Case law

Judgment of the EU Court of Justice of July 29, 2019, Case C-40/2017

“The operator of a website that features a Facebook ‘Like’ button can be a controller jointly with Facebook in respect of the collection and transmission to Facebook of the personal data of visitors to its website. By contrast, that operator is not, in principle, a controller in respect of the subsequent processing of those data carried out by Facebook alone.”



Judgment of the EU Court of Justice of September 24, 2019, Case C-136/17

“The ban on processing certain sensitive data categories also applies to search engine operators, having to weigh up the rights of the person who requests the deletion of references and the freedom of information of cybernauts.”

ECJ judgment passed on September 24, 2019

IV. Regulations, resolutions, recommendations, opinions and other

Information 2019/C 222/01 on the list of competent authorities that can directly consult the data entered in the second generation Schengen Information System, under article 31, no. 8 of (EC) Regulation 1987/2006 of the European Parliament and of the Council and article 46, no.8 of Decision 2007/533/JAI on the setting up, operation and use of the second generation Schengen Information System

Commission Communication 2019/C 229/01 – Technical guidelines on data protection according to (EC) Regulation 1107/2009 (phytopharmaceutical products)

(EU) Regulation 2019/1150 of the European Parliament and of the Council of June 20, 2019, promoting fairness and transparency for business users of online intermediation services

Opinion of the European Economic and Social Committee 2019/C 240/08 on the “Proposal for a Council Directive amending Directive 2006/112/EC as regards introducing certain requirements for payment service providers” [COM(2018) 812final – 2018/0412(CNS)] and on “Proposal for a Council Directive amending Council Directive 2006/112/EC of 28 November 2006 as regards provisions relating to distance sales of goods and certain domestic supplies of goods” [COM(2018) 819 final – 2018/0415(CNS)]

Opinion of the European Economic and Social Committee 2019/C 240/12 on the “Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions — Coordinated Plan on Artificial Intelligence” [COM(2018)795 final]

Information 2019/C 309/09 on electronic identification schemes notified under Article 9(1) of Regulation (EU) 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market

Amendment to Directive (EU) 2017/2455 issued by the Council on December 5, 2017, amending Directive 2006/112/EC and Directive 2009/132/EC regarding certain value-added tax obligations for supply of services and distance sales of goods



Commission Implementing Regulation (EU) 2019/1583 of September 25, 2019, amending Implementing Regulation (EU) 2015/1998, establishing detailed measures for implementing the common basic standards on aviation security relating to cybersecurity measures

Commission Notice 2019/C 323/04 – Guidance on interpreting and applying Council Directive 93/13/EEC on unfair terms in consumer contracts



Contact

Cuatrecasas, Gonçalves Pereira & Associados,
Sociedade de Advogados, SP, RL
Sociedade profissional de responsabilidade limitada

Lisboa

Praça Marquês de Pombal, 2 (e 1-8º) I 1250-160 Lisboa I Portugal
Tel. (351) 21 355 3800 I Fax (351) 21 353 2362
cuatrecasasportugal@cuatrecasas.com I www.cuatrecasas.com

Porto

Avenida da Boavista, 3265 - 5.1 I 4100-137 Porto I Portugal
Tel. (351) 22 616 6920 I Fax (351) 22 616 6949
cuatrecasasporto@cuatrecasas.com I www.cuatrecasas.com

For additional information about the contents of this document, please get in touch with your usual contact at Cuatrecasas.

© Cuatrecasas, Gonçalves Pereira & Associados, Sociedade de Advogados, SP, RL 2019.
The total or partial reproduction is forbidden. All rights reserved. This communication is a selection of the news and legislation considered to be relevant on reference topics and it is not intended to be an exhaustive compilation of all the news of the reporting period. The information contained on this page does not constitute legal advice in any field of our professional activity.

Information about the processing of your personal data

Data Controller: Cuatrecasas, Gonçalves Pereira & Associados, Sociedade de Advogados, SP, RL ("Cuatrecasas Portugal").

Purposes: management of the use of the website, of the applications and/or of your relationship with Cuatrecasas Portugal, including the sending of information on legislative news and events promoted by Cuatrecasas Portugal.

Legitimacy: the legitimate interest of Cuatrecasas Portugal and/or, where applicable, the consent of the data subject.

Recipients: third parties to whom Cuatrecasas Portugal is contractually or legally obliged to communicate data, as well as to companies in its group.

Rights: access, rectify, erase, oppose, request the portability of your data and/or restrict its processing, as described in the additional information.

For more detailed information on how we process your data, please go to our [data protection policy](#).

If you have any questions about how we process your data, or if you do not wish to continue receiving communications from Cuatrecasas Portugal, we kindly ask you to inform us by sending a message to the following email address data.protection.officer@cuatrecasas.com.