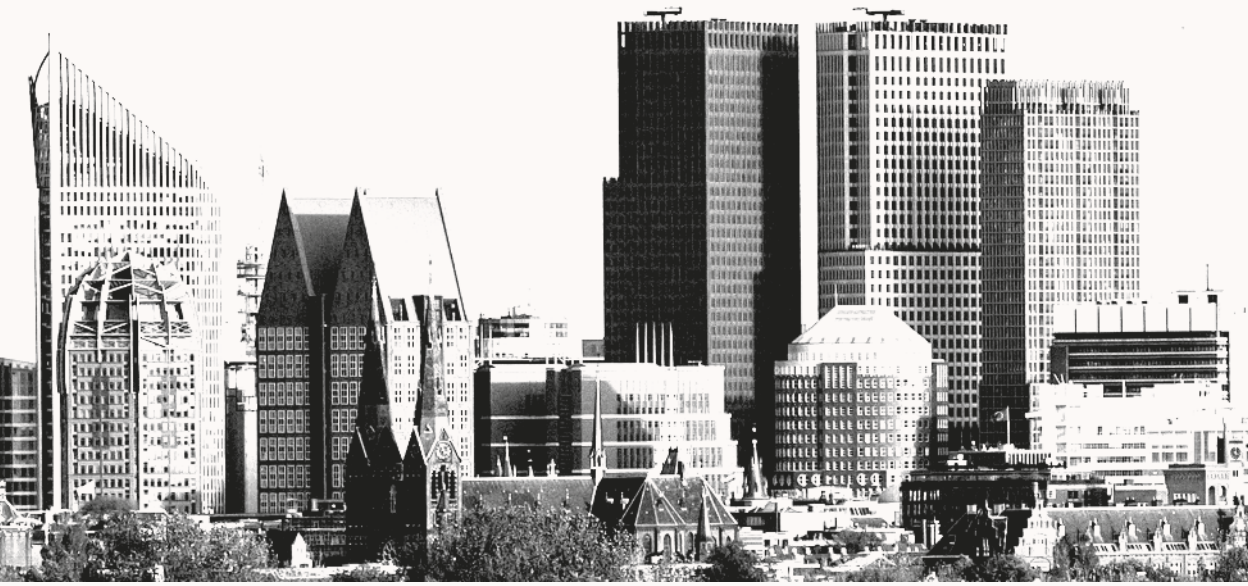
FIDE XXIX Congress The Hague 2020

THE NEW EU DATA PROTECTION REGIME: SETTING GLOBAL STANDARDS FOR THE RIGHT TO PERSONAL DATA PROTECTION

THE XXIX FIDE CONGRESS IN THE HAGUE
2020 CONGRESS PUBLICATIONS

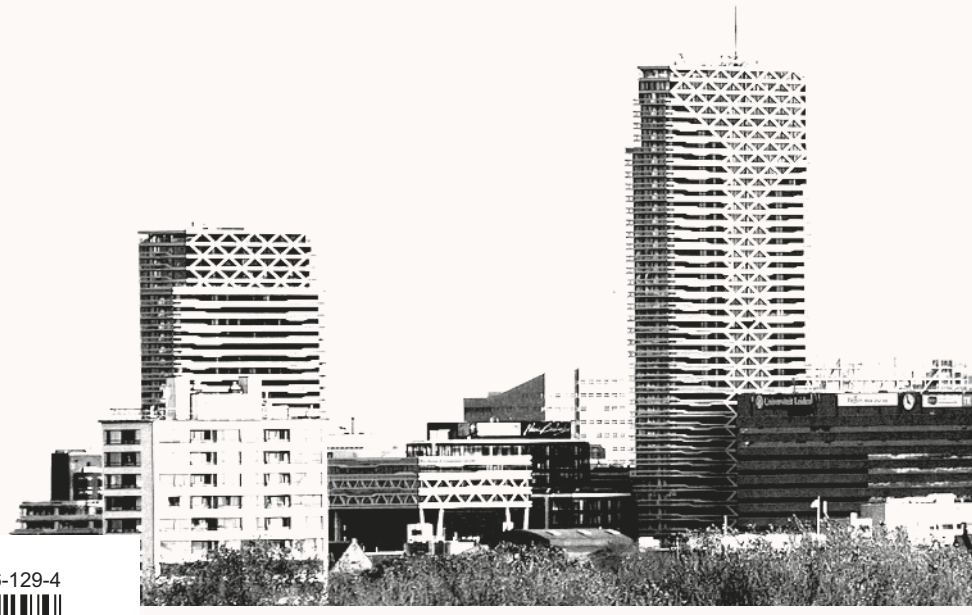
VOL. **2**



Jorrit J. Rijpma (Ed.)

eleven
international publishing

The proceedings of the XXIX FIDE Congress in The Hague in 2020 are published in four volumes. This book (Vol. 2) contains the reports of the General Rapporteur (Orla Lynskey), the Institutional Rapporteurs (Herke Kranenborg and Anna Buchta) and the National Rapporteurs on Topic 2: The New EU Data Protection Regime: Setting Global Standards for the Right to Personal Data Protection.



ISBN 978-94-6236-129-4

FIDE XXIX Congress The Hague 2020

The New EU Data Protection Regime

The New EU Data Protection Regime

Setting Global Standards for the Right to Personal Data Protection

Le nouveau cadre reglementaire de l'UE en matiere de protection des donnees

L'enonciation de normes mondiales pour le droit a la protection des donnees personnelles

Das neue EU Datenschutzregime

Setzen globaler Standards für das individuelle Recht auf Datenschutz

The XXIX Congress in The Hague, 2020
Congress Publications Vol. 2
Editor: Jorrit J. Rijpma
General Rapporteur: Orla Lynskey
Institutional Rapporteurs: Anna Buchta & Herke Kranenborg

eleven
international publishing

Published, sold and distributed by Eleven International Publishing
P.O. Box 85576
2508 CG The Hague
The Netherlands
Tel.: +31 70 33 070 33
Fax: +31 70 33 070 30
e-mail: sales@elevenpub.nl
www.elevenpub.com

Sold and distributed in USA and Canada
Independent Publishers Group
814 N. Franklin Street
Chicago, IL 60610
USA
Order Placement: (800) 888-4741
Fax: (312) 337-5985
orders@ipgbook.com
www.ipgbook.com

Eleven International Publishing is an imprint of Boom uitgevers Den Haag.

ISBN 978-94-6236-129-4

Printed in the Netherlands

Table of Contents

Portugal

Filipa Calvão and Clara Guerra[*]

A Setting the Scene

Question 1

In Portugal, the national legal instrument introduced to implement Regulation (EU) 2016/679 (General Data Protection Regulation, hereinafter "GDPR") is Law 58/2019, of 8 August 2019. It also amends Law 43/2004 of 18 August 2004, that rules the composition, organisation and functioning of the National Supervisory Authority (hereinafter "NSA").[1]

It should be stressed that the late publication of the national implementing law prevented Portugal from having its data protection legal framework completed. This can explain some lack of doctrine and of case-law, resulting from somehow limited practical application of the GDPR.

It identifies the NSA, providing for similar provisions to those who have been ruling the constitution and activity of this public authority for the past two and a half decades with the novelty of recognising the NSA financial autonomy and legal personality (articles 3 to 5 of Law 58/2019). Moreover, the Portuguese NSA is the public authority entitled to supervise and monitor the compliance with the GDPR, the Law 58/2019 «as well as further legislative and administrative provisions related to data protection, in order to ensure rights and freedoms of individuals in the context of personal data processing».[2]

To accredit certification bodies the law appoints the national accreditation body designated in accordance with Regulation (EC) 765/2008 (article 14(1) of Law 58/2019).

There are some provisions on Data Protection Officers, in particular on the designation by public authorities or bodies (articles 9 to 13 of Law 58/2019), and also a provision related to article 8 GDPR, determining the age threshold of 13 years old (article 16 of Law 58/2019).

---

* Filipa Calvão: Associate Professor, Faculty of Law (Oporto School), Catholic University of Portugal; Researcher, Católica Research Centre for the Future of Law; President of the Portuguese Data Protection Authority. Clara Guerra: Senior Consultant, Portuguese Data Protection Authority; Guest Lecturer, Faculty of Law, Catholic University of Portugal.

1 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, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.

2 Art. 4(2) of Law 58/2019 of 8 August 2019.

It also contains several provisions referring to the exercise of the right to remedies and liability (articles 32 to 35 of Law 58/2019).

It is important to highlight that, under recital 27 of the GDPR, the Portuguese law has extended to deceased persons the protection of personal data listed in article 9(1) of the GDPR and those related to private life, image and telecommunication (article 17 of Law 58/2019). On this aspect, the Portuguese legislator has partially reaffirmed the interpretation of the previous legal regimen on data protection based on the legal provisions of the Portuguese Civil Code that protect the personality of deceased persons (articles 71 and 80 of the Civil Code), just not covering personal data outside the special categories of data and outside data of a highly personal nature.

In what concerns the flexibilities provided for in the GDPR, apart from provisions related to the processing in the context of employment and health and genetic data (articles 28 to 30 of Law 58/2019), the Portuguese Law does not fully avail them.

In particular, the provision referring to the balance between data protection and freedom of expression and information does not provide for limits or specific guarantees, beyond those already reflected in the Portuguese Constitution (article 24 of Law 58/2019). In what concerns processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, it has derogated with no exception, and with poor guarantees, the rights referred to in articles 15, 16, 18 and 21 of the GDPR (article 31(2) of Law 58/2019). Also some rights provided for by the GDPR, such as the right to information provided by Article 13 and the right of access, are restricted by the national law in breach of the requirements stated by article 23 of the GDPR (article 20 of Law 58/2019).

Finally, there is a set of provisions on administrative fines that are in breach of the GDPR, concerning the infringements settled by article 83 (4) and (5), which were developed in articles 37 to 39 of Law 58/2019. On the one hand, the maximum amounts of administrative fines determined by article 83(4) and (5) of the GDPR are lowered, taking into account the nature of the controller or processor, in particular if it is an individual or a small and medium enterprise; on the other hand, the infringements that have a negligent character cannot be sanctioned by the NSA unless, after an "advise" to correct the situation, the infringements continue; in some cases negligent infringements are not sanctioned at all (e.g. infringement of the principles provided by article 5 of the GDPR).

In what concerns the Law 58/2019, the Portuguese SA has given a very critical opinion on its draft proposal during the legislative proceeding and has taken the resolution not to apply in its future decisions the provisions that are clearly in breach of the GDPR.[3]

3 Deliberação/2019/ 494 of 3 September 2019 of the Comissão Nacional de Proteção de Dados (hereinafter "CNPD"), www.cnpd.pt/bin/decisoes/decisoes.asp?primeira_escolha=2019&segunda_escolha=20. All webpages referred to were visited on 9 February 2020.

Question 2

The Portuguese Constitution differentiates, since its approval on 2 April 1976, the right to respect for private life and the right to data protection (articles 26 and 35, respectively), being the first written Constitution in the world to recognise the protection of personal data as a fundamental right.

Beyond the legal protection ensured by national civil law (article 80 of the Civil Code of 1966), the Portuguese Constitution recognises the respect for private life as a fundamental right in article 26(1) and (2) and provides for specific guarantees in the context of telecommunication in article 34(4).[4]

Article 35, with the title 'Use of computerized data', of the Portuguese Constitution of 1976 provided for a set of fundamental rights related to data processing through automated means, that intended to ensure the right to informational self-determination.[5],[6]

Later, by the revision of the Constitution that occurred in 1997 in order to adjust this article to Directive 95/46/EC, the material scope of this provision was extended to the processing of personal data other than by automated means.[7]

It is worthwhile mention that since its first wording, article 35 (3) relates both fundamental rights, specifying that private life is, among other personal data (sensitive data), subject to reinforced protection.[8]

Hence, the Charter of Fundamental Rights of the European Union (hereinafter "Charter") has not had such a significant impact in Portugal as it might have had in other Member-States.

Nevertheless, the Charter is frequently invoked for supporting the guarantee of the right to data protection before national courts as well as by the NSA, in particular in its written advices on drafts of legislative and administrative measures as well as in its concrete

4 Rectius, the Portuguese Constitution provides for the right to the *intimacy* of private and familiar life. Though this formulation seems to be more restricted than the one of the Charter of Fundamental Rights of the European Union, the truth is that the Constitutional Court has affirmed a broad interpretation of that right, covering also a patrimonial dimension of private life – see judgments 278/95 and 355/97, in www.tribunalconstitucional.pt/tc/acordaos/.

5 J.J. Gomes Canotilho &Vital Moreira, *Constituição da República Portuguesa Anotada*, 4th ed., Coimbra, Coimbra Editora, 2007, vol. I, pp. 551-556.

6 P. Ribeiro de Faria, 'Anotação ao artigo 35.º', *in* Jorge Miranda & Rui Medeiros, *Constituição Portuguesa Anotada*, 2nd Ed, Coimbra, Coimbra Editora, 2010, Vol. I, pp. 779-801.

7 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with the regard of the processing of personal data and on the free movement of such data [1995] OJ L281/31.

8 Explaining the history of this constitucional provision, see Joaquim Seabra Lopes, 'O artigo 35.º da Constituição: da génese à atualidade e ao futuro previsível', in *Forum de Proteção de Dados*, n.º 2, Jan. 2016, pp. 14-51, www.cnpd.pt/bin/revistaforum/forum2016_2/index.html. See also Alexandre Sousa Pinheiro, *Privacy e protecção de dados pessoais: a construção dogmática do direito à identidade informacional*, Lisboa, AAFDL, 2015, pp. 695 ss.

decisions regarding the balance between that fundamental right and other rights or interests in conflict.

B The Reception of Substantive GDPR Provisions in the National Legal Order

Question 3

Before 2018, the national law that transposed Directive 95/46/EC (Law 67/98, of 26 October 1998) provided for the need to obtain a prior authorisation from the NSA to process sensitive data, as well as to further process data for new purposes. Therefore, only under GDPR application have data controllers started applying themselves directly these principles and processing data accordingly to their own assessment.

In this new context, most data controllers reveal difficulties in assuming this new task, especially in interpreting and applying the principles of purpose limitation and data minimisation.

With regard to purpose limitation principle, data controllers tend to a generous evaluation of the compatibility test between the original and the new purposes. In particular, when controllers are public bodies there has been an intense reaction from civil society signalizing an abuse in some cases of further processing for new purposes, which led to the correction of the processing or simply a more careful and rationalized decision for future processing of data.

As to the data minimisation principle, data controllers tend to have increased difficulties in implementing it. The same occurs with the implementation of the storage limitation principle. Actually, praxis reveals a tendency to collect and store more data than necessary for the specified purpose of the processing as well as a difficulty to determine the adequate period of retention and to justify the option made.

For a better application of those principles, the Portuguese SA issued guidelines on specific kinds of data processing – most of them still under the Law that transposed Directive 95/46/EC – developing and adjusting the interpretation made by Article 29 Working Party and by the European Data Protection Board (EDPB), to the specificities of the national legal order, in particular in some sectors of activity.

Furthermore, the NSA has issued decisions advising moderation on the reuse of data for other purposes than the one for which personal data had been collected.

Although so far there are no judgements by the Portuguese Courts under the GDPR, as the principles remain unchanged in relation to Directive 95/46/EC, the following should be noticed: domestic Courts do not ignore the guidelines of Article 29 Working Group nor of the Portuguese SA, given that the parties involved in the process do usually invoke

them in their submissions, and in most cases share the same perspective; in spite of that, the case-law is not always in accordance with the interpretation of the NSA.[9]

Question 4

As already pointed out, there are no judgements by the Portuguese Courts under the GDPR until now, so the national Courts' interpretation on the legal basis for data processing is related to the legal basis provided for by the law that transposed Directive 95/46/EC (Law 67/98), which is similar to the conditions of lawfulness provided for by the GDPR.

In this context, the case-law shows some discrepancies on the evaluation of the attributes of consent, particularly with regard to the legal requirement of specific consent (e.g., consent given by a person for access to his/her health data by insurance companies).[10]

With respect to legitimate interests there are not many judicial decisions, in part because the balance between data protection and other interests, like administrative transparency or the exercise of a right in a judicial process, is done by the Courts on the grounds of other specific laws. Furthermore, regarding legitimate interests in the digital environment, although there are some interesting judgments on the disclosure and on the reuse of personal data in the context of social networks, the majority of the case-law focuses on the right to respect of private life and not on the right to data protection and its specific legal regimen[11].

On balancing of interests, it should be highlighted a judgement by the Court of appeal, forbidding parents to disclose photographs or any other information that could lead to the identification of their child in social media, on the grounds of the prevalence of private life and data protection over the freedom of expression of the parents, in the name of the superior interest of the child.[12]

9 About the proportionality of the data retention period, see the judgment of the Supreme Administrative Court of 21 March.2019, Proc. No. 220/17, at www.dgsi.pt.

10 See the judgment of the Supreme Administrative Court of 08 August 2018, Proc. No. 0394/18, at www.dgsi.pt,. Concerning the access by a third party to health data, the Court ruled that it should only be given access to the data expressly covered by the statement of consent. About consent, see also Alexandre Sousa Pinheiro, 'Anotação ao artigo 4.º, 11)', *in* Alexandre Sousa Pinheiro (Ed.) *Comentário ao Regulamento Geral de Proteção de Dados*, Coimbra, Almedina, 2018, pp. 166-173.

11 Within this context, following the criteria of the expectation of privacy, see, for all, the judgment of *Tribunal da Relação do Porto* (an intermediate court of appeal) of 08 September 2014, Proc. No. 101/13.5TTMTS.P1, at www.dgsi.pt.

12 Judgment of *Tribunal da Relação de Évora* (an intermediate court of appeal) of 25 October 2015, Proc. No. 789/13.7TMSTB-B.E1, in www.cnpd.pt/bin/revistaforum/forum2016_2/index.html.

Question 5

In regard to the validity of personal data as 'counter-performance' for the provision of digital content, this issue has been debated in Portugal, mainly in the context of conferences and seminars.[13]

Recently the new Law 58/2019 has contributed to this debate through a provision that seems to admit that the legitimacy of processing personal data *necessary* for the performance of a contract might be found on consent. Actually, article 61(2), regarding data processing that existed prior to the application of the GDPR, intends to ensure that consent fulfils the attributes provided for by article 4(11) of the GDPR, determining the end of a contract to which the data subject is party if the consent is not in accordance with the GDPR. Although this provision is not necessarily headed to contracts on digital services or goods, yet it has surely the consequence of generating confusion on an issue that seemed relatively pacified by the GDPR.

It should also be highlighted that the NSA has decided not to apply in concrete cases that national provision on the ground that is in breach of articles 4(11) and 6(1)(a) and (b) of GDPR.

Question 6

In what concerns the rights provided by the GDPR to data subjects, the Portuguese Law is quite restrained. Actually, Portugal did not introduce so far any national legislative measure concerning automated decision-making, making use of the possibility provided by article 22(2)(b) of the GDPR.

Question 7

With regard to the right to erasure towards search engines, the NSA has handled some requests from data subjects in order to have their right guaranteed, following standard answers received from the data controllers denying to de-list the results presented when searching by a name, always invoking public interest in providing such information, regardless of the context or the notoriety of the person concerned.

13 About the difficulties to legitimate the colletion of personal data in the digital environment under the GDPR, see also A. Leal Alves, 'Aspetos jurídicos da análise de Dados na Internet (Big Data Analytics) nos setores bancário e financeiro: proteção de dados pessoais e deveres de informação' in A. Menezes Cordeiro et al. (Eds), *FinTech. Desafios da Tecnologia Financeira*, Coimbra, Almedina, 2017, pp. 75-150.

In general, the NSA did not recognize the arguments of the companies, for going much beyond the interpretation of the CJEU ruling in the Case *Google Spain*; therefore, it decided in favour of the data subjects and it issued deliberations ordering the de-listing.[14,15]

The search engines either complied with the NSA decision or challenged it in the court, there being no apparent reason for the different ways taken. Those cases are still pending at the national courts.

Still in respect to the right to erasure, national law implementing the GDPR has notably introduced a provision on how this right can be ensured when personal data is published in the official journal.

It states that the right to erasure of personal data published in the official journal has an *exceptional nature* and can only be applied in the conditions laid down by article 17 of the GDPR in the cases where it is the only way to safeguard the right to be forgotten, after due balance of the interests at stake. This is done through the deindexation of personal data from the search engines, but always without erasure from the official publication (article 25(4) and (5) of Law 58/2019).

It is also determined by this law that, in case of publication of personal data by the official journal, the data controller is the body requesting the publication (article 25(6) of Law 58/2019).

Definitely, there is no right to erasure from the official journal, but a right, in certain circumstances, not to have the personal data published by the official journal processed by search engines. This is exercised not directly towards the search engines, as data controllers, but has to be exercised via the official journal which is the body that controls the online publication and is able to make the deindexation, yet not being the data controller.

Question 8

About national legislative measures to reconcile the right to data protection with the right to freedom of expression, Portugal did not really regulate how this balance could be achieved nor did introduce any actual derogations. Article 24 of Law 58/2019 disposes that the GDPR and national rules on data protection are without prejudice of the freedom of expression and of the freedom of information and of the press. It provides in general terms that the exercise of the right to information shall respect the principle of human dignity

14 Judgment of 13 May 2014, in Case C-131/12, *Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* (Google Spain), ECLI:EU:C:2014:317.

15 About the grounds for the decisions of the Portuguese SA, see J. Marques, 'Direito ao esquecimento. A aplicação do acórdão Google pela CNPD', in *Forum de Proteção de Dados*, No. 3, July, 2016, pp. 48-55, in www.cnpd.pt/bin/revistaforum/forum2016_3/index.html.

and the personality rights, in particular whenever discloses special categories of data or personal data of deceased persons.

Then a specific provision affords special protection to data subjects' addresses and contacts, expressly providing that the right to freedom of information does not legitimate such disclosure, unless when data is already of public knowledge (article 24(4) of Law 58/2019).

The GDPR implementing law introduced though a clear distinction between data processing within freedom of expression and data processing for journalistic purposes, when requiring that in the latter case such processing shall comply with national law on access and exercise of the professional journalism.

In Portugal there is already specific legislation regulating the activity of the press and other social communication means, including journalists' activity, and there is a dedicated independent regulator to monitor compliance with such legal framework. However, such legislation does not contain any provisions on personal data protection or provide for the exercise of GDPR data subjects' rights.

It should be noted, in this context, that the Press Law[16] provides that the freedom of the press is only limited by the Constitution and the law, in order, namely, to ensure the accuracy and objectivity of the information and to guarantee the rights to good reputation, intimacy of private life and image.

Apart from these general restrictions, which can be related to the processing of personal data, there are no other provisions intended to strike the balance between data protection and the freedom of expression and information.

C Domestic Enforcement of Data Protection Law

Question 9

In what regards the national enforcement of data protection law, it should be underlined that the Portuguese data protection supervisory authority is Comissão Nacional de Proteção de Dados (hereinafter «CNPD»).[17]

It is an independent administrative legal body with powers of authority and administrative and financial autonomy that operates within the Parliament. Its composition, statute and staff are approved by law of the Parliament.

The CNPD is a public legal person directed by a collegiate body, composed of seven members of recognized merit and integrity: one President elected by the Parliament; two

16 Art. 3 of Law 2/99, of 13 January 1999.

17 Arts. 3 to 6 of Law 58/2019 and Law 43/2004, amended by Law 58/2019.

members elected by the Parliament by Hondt's highest average rule; one judge appointed by the Judiciary Superior Council and one magistrate from the Public Prosecutor's Office appointed by its own Superior Council; two members appointed by the Government.

The members have a five-year mandate that can be renewed twice. They take office before the President of the Parliament. All activities, paid or unpaid, are considered incompatible with the NSA membership, with the exception of teaching in the University and researching. The CNPD acts with independence when fulfilling its tasks and exercising its powers.

The CNPD is provided with its own staff, only bound by the general rules governing public administration.

The national law implementing the GDPR provides for the following additional competences for the NSA: to issue non-binding opinions on draft legal instruments in preparation at European or international institutions related to personal data protection; to monitor the compliance of the GDPR and other legal provisions on the protection of personal data and of the rights, freedoms and guarantees of the data subjects, as well as to correct and sanction any non-compliance; to define criteria allowing to densify the concept of 'high risk' referred to in article 35(4), in connection with the list of data processing operations requiring a Data Protection Impact Assessment; to draft and submit to the EDPB the criteria for the accreditation of the monitoring bodies for codes of conduct and of the certification bodies, pursuant articles 41 and 43 of the GDPR; to cooperate with the National Accreditation Body (IPAC, IP), entrusted with the task provided by article 43(1)(b) of the GDPR, in particular in the definition of additional requirements for accreditation.

In what concerns enforcement under the GDPR, for the period 25 May 2018-31 July 2019, the NSA presents the following statistics:[18]

- Number of investigation proceedings (resulting from complaints, referrals from other national authorities and the NSA's own initiative): 1075
- Number of data breaches notifications (article 33 GDPR): 326
- Number of inspections on the spot: 325
- Number of organisations (public and private) to which fines were applied: 5
- Total amount of the fines applied: ± 425 000 euro

Besides the enforcement activity carried out at national level, the consistency mechanism provided by the GDPR has brought a new line of work requiring involvement of NSAs upon the likelihood of data subjects in that Member State being affected by data processing even when there is no establishment of the controller in that territory. Consequently,

18 These figures were provided by CNPD for the 1st anniversary of GDPR application and then updated with reference to the end of July, in a time frame of 14 months still with no national GDPR implementing law.

additional efforts on enforcement are required. In spite of being not converted into these statistics, they have a real impact on the enforcement activity at national level.

Question 10

As to the strategy of the NSA for complaints-handling, it is important to recall that the right to data protection is a fundamental right, not only recognised by the Charter but also by the Portuguese Constitution.

Therefore, there is a legal obligation to ensure to each individual that his/her rights are guaranteed. In view of the possible great amount of complaints, several strategies can be envisaged to handle complaints in an effective manner, such as sorting them according to similarity, planning inspection activities having due account of the main or recurrent problems detected or redefining internal working methods to cope with new scenarios.

However, the Portuguese SA cannot, according to the national legal order, ignore complaints based on an assessment of minor pertinence of the complaint. In fact, all admissible complaints have to be dealt with, according to the law, since it imposes such obligation to the NSA leaving no margin of discretion.

Though prioritization is indispensable, mainly because of the lack of resources of the NSA to fully comply with its tasks, it cannot lead to setting aside a case where a fundamental right of an individual is or might be at risk. In that sense, the effectiveness in the action of the NSA cannot be affirmed with prejudice to fundamental rights.

Question 11

Law 58/2019 adds sanctions to those explicitly provided for by the GDPR, maintaining a tradition of recognising criminal relevance to some infringements of data protection provisions: further processing of personal data for a purpose incompatible with the initial purpose; undue access to personal data; invalidation or destruction of personal data; data deviation; entry of false data; violation of the duty of secrecy; non-compliance with an order of the NSA (articles 46 to 52 of Law 58/2019).

Besides criminalising those conducts, national law also provides for administrative fines for some infringements of the GDPR not covered by article 83(4) and (5) of the GDPR: the infringement of articles 10 and 41(4); and the monitoring of codes of conduct by bodies not accredited by the NSA – articles 37(1)(e) and 38(1)(q) and (r) of Law 58/2019.

The Law, in article 37(1)(l), also sanctions with administrative fines the infringements of the limits and conditions stated on its chapter VI, relating to specific processing operations under articles 85 to 89 of the GDPR.

As mentioned supra, Law 58/2019 has provisions that are in breach of the GDPR, concerning the infringements settled by article 83(4) and (5). The Portuguese legislator determined different maximum amounts of administrative fines from the ones provided in the GDPR, depending on the controller or processor being an individual or a small and medium enterprise – articles 37 (2) and 38(2). Besides, the national implementing law prevents the NSA to sanction negligent infringements unless, after an "advise" to correct the situation, the infringements continue – article 39(3). Though having replicated the list of infringements provided by article 83(4) and (5), it has omitted the negligent infringement of the principles provided by article 5 of the GDPR, reducing the provision to an intentional infringement.

In what regards the exercise of corrective powers by the Portuguese SA, it should be noticed that such powers are not, in fact, new in the national legal order. The previous data protection law (Law 67/98) already endowed the SA with corrective powers, specifying the power to apply administrative fines. The only difference has to do with the legal framework of the administrative fines, which is now much more impressive than the one provided by the Portuguese law twenty years ago.

Despite the fact that the national law that implements the GDPR is in force only since 9August 2019, the CNPD has been exercising the powers provided by the GDPR on the ground that the Law 67/98 had not been implicitly revoked in full, keeping in force the national provisions that did not contradict the GDPR, in particular the one that appointed the CNPD as national SA.

Therefore, during the past year the CNPD has applied, under the GDPR, several corrective measures mainly to data controllers, among which stands out four decisions sanctioning data controllers.[19]

Question 12

Article 82 of the GDPR, providing data subjects for a right to receive compensation for material or non-material damages as a result of an infringement of the GDPR, does not represent a real innovation in the Portuguese legal order.

Indeed, the previous data protection law (Law 67/98) already provided for the right to compensation, and it was interpreted combined with further legal provisions that specified the coverage of non-material damages.

Article 496 of the Civil Code (of 1966) and article 3 of the Rules of non-contractual civil liability of State and other Public Entities, approved by Law 67/2007, of 31December

19 See Deliberação 984/2018, in www.cnpd.pt/bin/decisoes/Delib/20_984_2018.pdf and Deliberação/2019/21, Deliberação/2019/207 and Deliberação/2019/222, www.cnpd.pt/bin/decisoes/decisoes.asp?primeira_escolha=2019&segunda_escolha=20.

2007, provide for the compensation for non-material damage, although limiting it to the damages that, for its gravity or seriousness, deserve legal protection. This last precision, explicitly stated in article 496 of the Civil Code, has been interpreted as to exclude the minor harm – and this is the only aspect of national law that may raise some difficulties in ensuring the implementation of article 82 of the GDPR in accordance with the case law of the CJEU, according to which "Reparation for loss or damage caused to individuals as a result of breaches of Community law must be commensurate with the loss or damage sustained so as to ensure the effective protection for their rights".[20] However, there are some Portuguese authors that consider this national legal requirement as a short add, since it has to be evaluated in each concrete case.[21]

Hence, Portuguese Courts have long condemned those who inflicted non-material damages, taking into consideration not only physical pain and emotional suffering, but also damage caused by the disclosure of facts related to private life.[22]

More recently there are judgments recognising the right to receive a compensation for the infringement of provisions that protect personal data.[23]

In what concerns the criteria for calculating such damages, the case-law follows an "equity judgment", taking into account the degree of fault as well as the economic situation of both the one who inflicted the damage and the injured person.[24]

Question 13

Concerning the information and power asymmetries between data controllers and data subjects and the purpose of the EU legislator to mitigate them by providing for the possibility of representative actions pursuant to article 80 of the GDPR, it is important to

20 Judgement of 5 March 1996 in Joined Cases C-46/93 and C-48/93, *Brasserie du Pêcheur SA v. Federal Republic of Germany and The Queen v. Secretary of State for Transport, ex parte Factortame Ltd and Others,* ECLI:EU:C:1996:79, para 82.

21 See M. Rebelo de Sousa & A. Salgado de Matos, *Direito Administrativo*, 2nd ed., Lisboa, D. Quixote, Ed., 2009, Vol. III, p. 496.

22 See, for instance, the judgment of the Supreme Court of Justice of 3 November 2016, Proc. No.323/12.6TVLSB,L2.S1, recognizing the right to compensation for non-material damages caused as a result of negligent breach of the duty to store a video that registered an intimate moment between the legitimate holder of the video and the person injured.

23 See the judgement of the Supreme Court of Justice of 16 October2014, Proc. No.679/05.7TAEVR.E2.S1, in a case where privacy and reputation of several data subjects (civil servants) was at stake as a result of the disclosure of personal data by the intentional action of a public office holder (notice that such data disclosures were judged, in the prior criminal law suit, as infringements to criminal law provisions related to data protection).

24 See the judgement of the Supreme Court of Justice of 4 May2010, Proc. No. 256/03.7TBPNH.C1.S1, at www.dgsi.pt.

recall that the new legal framework is very recent, being still difficult to assess potential trends in civil society in this regard.

Portugal does not have in general a high level of involvement of NGOs in representative actions. However national administrative law and administrative process law recognise to associations their legitimacy to defend 'collectively' the individual interests of its members provided that those interests are covered by the object matter or scope of the association. This possibility has been availed by unions to complain or report to the NSA infringements of data protection legal regimen, but seems insufficient – without a mandate from the data subject – to the exercise of the right to redress.

National law implementing the GDPR does not further develop Article 80 (1) of the GDPR, only admitting representation through a mandate of the data subject (Article 35 of Law 58/2019). Nevertheless, it is predictable that such kind of actions may significantly increase in the near future.

Question 14

In what concerns the intervention of further regulatory agencies or public authorities in data processing related complaints, it should be highlighted that in Portugal the supervision of data protection issues has been centralised in the CNPD for the last 25 years. Even in the e-Privacy legislation, where there are shared competences with the telecom regulator, the competences are well distinguished and data protection matters are only assigned to the NSA.[25]

In view of that, other regulators or authorities usually forward to the NSA complaints related to data protection and, moreover, they report to the NSA facts found in their own investigations, such as in the employment context, economic activities, consumer protection, financial sector and so forth.

The NSA has also a cooperation mechanism with the Ombudsperson in place for several years, for the exchange of information and complaints handling. Furthermore, there are some bilateral discussions with public bodies dealing with convergent matters to data protection and privacy, such as ethics, scientific research, e-voting and the national statistic system. Especially after the GDPR, informal cooperation between the NSA and Regulatory Agencies has increased, due to the consciousness of the importance to avoid contradictions in its respective guidelines or administrative measures.

25 Law 41/2004, of 18 August 2004, as amended by Law 46/2012, of 29 August 2012.

D Data Processing for National Security Purposes

Question 15

There is no legal definition of 'national security', but it is commonly perceived that national security is ensured by intelligence services, due to their tasks, and not by law enforcement authorities. Consequently, as there is a constitutional prohibition for the intelligence services to carry out any criminal prevention or investigation, the scope of the application of Directive 2016/680 and its transposition into national Law 59/2019, of 8 August 2019, make it clear that excluding national security means in Portugal excluding the intelligence services from the application of the Law Enforcement Directive (LED).[26,27]

The intelligence services (SIRP) are regulated by specific legislation and their activities are supervised by two different bodies: a parliamentary oversight commission and another body composed of magistrates to monitor some aspects of the data processing, including the exercise of the rights of the data subjects.

Being the right to data protection a fundamental right in Portugal since 1976, the first data protection law, dated from 1991 (Law 10/91 of 10 January 1991), already covered the law enforcement sector with the same data protection rules as the other public bodies and private organizations, with only two derogations concerning the right to information and the right of access which had specific provisions.

Actually, apart from the intelligence services, all other sectors were governed by the same data protection legal framework. Therefore, though the terminology might be confused, especially when used in European legal texts for different national contexts, the waters have been divided so far. It should be noted though that while excluding national security from its scope of application, the LED invokes 'national security' as one of the possible grounds to restrict data subjects' rights. The national law transposing the LED follows the same misleading legal provision, what might bring problems of interpretation and application of the law.

In what regards the national data retention law – Law 32/2008, of 17 July 2008 – its purpose is restricted to the prevention, detection and investigation of serious criminal infractions, by competent authorities, exactly like the subject matter and scope of the

26 'National security' is stated in art. 15 of the e-Privacy Directive (Directive 2002/58/EC) as meaning «State security». Without giving a definition, the European legislator clearly intended to determine the scope of national security.

27 Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L119/89.

Directive itself, which on the other hand refers to the national legislation. According to the Portuguese data retention law, only a limited number of listed law enforcement authorities can have access to the data retained to strike serious crime after a judicial warrant. Within this law, there is no use of data for national security purposes or access to data by intelligence services.[28]

Nonetheless, the national data retention law, after the CJEU ruling that invalidated the Data Retention Directive, is to be considered in breach of the Charter, regardless of the purpose for which the data is retained and further accessed.[29]

The NSA has expressed this view immediately after the invalidation of Directive 2006/24/EC and, after Tele 2 Judgement, it has deliberated not to apply the national data retention law for being in violation of EU Law.[30,31,32]

With the Portuguese Data Retention Law still in force, the Parliament passed a specific law to grant access by the intelligence services to the data retention database. The NSA gave a negative opinion during the legislative proceeding and the law was considered unconstitutional by the Constitutional Court in 2015, following a constitutionality prior check.[33,34]

A second law was passed, on which the CNPD issued a negative opinion as well. The Constitutional Court found it partially unconstitutional.[35,36]

In the meantime, the Ombudsperson requested the Constitutional Court to evaluate whether the national data retention law was in accordance to the Portuguese Constitution, including in what concerns the respect for the primacy of the EU law. Such request is still pending for assessment.[37]

---

28 Law 32/2008 is the Portuguese law transposing Directive 2006/24/EC. In spite of the Directive had been invalidated by the CJEU, the national law is still in force in Portugal.

29 Judgement of 8 April 2014 in Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Síochána, Ireland and the Attorney General, and Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and Others* (Digital Rights Ireland), ECLI:EU:C:2014:238.

30 Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC [2006] OJ L105/54.

31 Judgement of 21 December 2016 in Joined Cases C-203/15 and C-698/15, *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others* (Tele 2), ECLI:EU:C:2016:970.

32 Deliberação 641/2017 of the CNPD, www.cnpd.pt/bin/decisoes/Delib/20_641_2017.pdf and Deliberação 1008/2017 of the CNPD, www.cnpd.pt/bin/decisoes/Delib/20_1008_2017.pdf.

33 Parecer 51/2015 of the CNPD, www.cnpd.pt/bin/decisoes/Par/40_51_2015.pdf.

34 Judgement 403/2015 of the Constitutional Court, www.ribunalconstitucional.pt/tc/acordaos/20150403.html.

35 Parecer 38/2017 of the CNPD www.cnpd.pt/bin/decisoes/Par/40_38_2017.pdf.

36 Judgement 464/2019 of the Constitutional Court, www.tribunalconstitucional.pt/tc/acordaos/20190464.html.

37 Request from the Ombudsperson of 26 August 2019, www.provedor-jus.pt/?idc=32&idi=18045.

In spite of the national legal framework being clear in respect to the law enforcement and the national security activities, not affecting the scope of application of the LED, it is evident that there is an increasing trend to use data, primarily processed for commercial purposes, for law enforcement purposes in a massive and disproportionate way, and then becoming also available for access and further processing by national security agencies.