

/ NATIONAL DATA PROTECTION COMMISSION

OPINION/2019/41

I. Order

The Office of the Minister of the Sea sent the National Data Protection Commission (CNPd), for consideration, the draft decree-law that creates the Single Logistics Window (JUL), establishing the conditions of operation and access, its governance, management and operation and transposes Directive no. 2010/65/EU, of the European Parliament and of the Council, of 20 October, into the domestic legal system, on the declaration formalities required for ships upon arrival and departure from the ports of the States members, and which repeals Directive no. 2002/6/EC, of the European Parliament and of the Council, of 18 February.

The request made and the opinion issued now derive from the attributions and powers of the CNPD, as an independent administrative entity with powers of authority to control the processing of personal data, conferred by subparagraph c) of paragraph 1 of article 57 and by the no. 4 of article 36 of Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016 (General Regulation on Data Protection - RGPD), in conjunction with the provisions of no. Article 21(1) and Article 22(1), both of Law No. 67/98, of October 26, amended by Law No. 103/2015, of August 24 (Law of Personal Data Protection).

The assessment of the CNPD is limited to the rules that provide for or regulate the processing of personal data.

II. appreciation

The primary objective of this draft decree-law is to establish, at the national level, solutions for declarative facilitation by those who use national ports. The proposal for a European regulation on this matter, which has already been voted on by the European Parliament¹, and which should be published shortly, precisely points to the simplification of reporting obligations in this area². Furthermore, in addition to this facilitation, the text of the future regulation also includes the need to guarantee the interoperability of the flow management systems (of people, cargo and ships) in European ports.

¹ Agreed text available at http://www.europarl.europa.eu/doceo/document/TA-8-2019-0434_EN.html#title2.

² Cf. recital 19 of the aforementioned future regulation.

1 v.

r

It should be noted that, since Directive 2002/59/EC, in the field of ship traffic control in the EU, there has been a focus on systems that promote and make this interoperability effective.

In the Portuguese context, the most relevant of the novelties brought by this draft diploma is the expansion of declarative facilities and centralization of information to other means of transport, in this case, road and rail, proceeding to the standardization of models and obligations of information reporting on the so-called Janela Única Logística, a platform that now succeeds the Janela Única Portuária, whose legal framework began with Decree-Law No. 370/2007 of 6 November.

This new platform "is mandatory for the presentation of declaration formalities and for the management of information flows associated with the planning, execution and monitoring of the movement of means of transport and goods between the nodes of the transport chain that use the ports". national ports for import, export or transshipment, or in any specific circumstance that requires the use of a national port." (cf. article 3, paragraph 2). 3 and 4 of article 3 of the project: Maritime transport of people and goods through national ports; Transport of goods along logistical chains that use national ports; Transport of passengers by sea or river; Cruise traffic and management of marinas and recreational ports; Maritime tourism activities, including river traffic management; Services provided in fishing ports, including those relating to export and import of fish; Execution of declaration formalities and procedures associated with border control in international areas within the jurisdictional areas of national ports. It is prescribed, for all "Public and private entities that intervene in the JUL [the duty to] act in close collaboration, making the best efforts towards the concertation of interests, namely within the scope of the National Commission for the Simplification and Digitization of Transport and Logistics created by the present decree-iei, and in the coordinated development of information systems within the competence of each of the parties' (cf. article 4, no. 5 of the project). technological platform the natural and legal persons, public and private, to which this decree-law applies, in accordance with the provisions of article 11, paragraph 1.

A. Prior note

The draft decree-law is not clear about the existence of interconnections of different databases in order to allow the operationalization of the many capabilities described in article 9, paragraph 2. However, the need to make this platform compatible with the “national component of the SafeSea Net system concerning the implementation of Directive no. integrating the information derived, namely, from the positioning of ships and from the declarative acts carried out in the ports through the JUP’ (cf. do not allow the CNPD to make any judgment on their technical robustness or legal suitability).

It would be important, in view of the above, that the future decree-law can discriminate these interconnections (if any) and that they become the subject of regulation to guarantee the essential aspects of security and resilience of the communication networks in question.

B. Notes on the data protection regime

There is a generic clause in paragraph 4 of article 5 (General principles for the functioning of the JUL) which provides: “Without prejudice to the access to personal data provided within the scope of the JUL to the competent authorities, the confidentiality of commercial information is guaranteed and other sensitive information shared in the JUL, and the adequate treatment of such personal data is also ensured for the purposes set out in this decree-iei.” In itself, the wording of this number is not an obstacle to the implementation of the data protection regime, but the way in which personal data and “commercial data and other sensitive information” are included sets the tone of the draft decree-law, in which the matter related to the fundamental right, provided for in article 35 of the Constitution of the Portuguese Republic, seems to be addressed

3 As is also apparent from other passages in the preamble: “with a view to integrating maritime information on a single platform, all national and international systems whose information is necessary for the operation of this platform are interconnected with the JUL”.

AV. D. CARLOS I, 134 - 1

1200-651 LISBON j WWW.CNPD.PT | TEL: +351 213 928 400 | FAX: +351 213 976 832

Process PAR/2019/39

2v.

as an accessory or complementary dimension of the remaining information dealt with within the framework of the JUL.

As for the specific point of the protection of personal data, the project has its own article (Article 15), and two others carry

relevant dimensions linked to the fulfillment of fundamental obligations inscribed in the GDPR (Articles 16 and 17).).

- Responsible for the treatment

In this first article dedicated to regulating the processing of personal data in the context of this project, it is noted that those responsible for the processing⁴ of data entered in the JUL are "The ACN [National Competent Authority - the Directorate-General for Natural Resources, Security and Services Maritimes] and the A CL [Local Competent Authorities - port administrations], in accordance with the responsibilities defined in article 8'. The designation of these entities can be seen if we look at the provisions of paragraph 3 of article 9 of the project: "In order to ensure full compliance with legislation, as well as procedures aimed at increasing the effectiveness and efficiency of the means of transport and logistics chains associated with the maritime-port sector, the governance, management and operation of JUL are responsible for: a) CN with regard to national policies and decisions and technological solutions that make up the National Layer of JUL; b) To ACL with regard to other JUL's technological solutions. As they are responsible for complying with this legislation and making JUL operational, the natural consequence of this function would be precisely the attribution of the status of controllers, even because, in addition to the functional management of the platform, the realization of the rights of the data subjects cannot fail to correspond to this statute whoever is materially qualified to determine and manage the cycle the lifetime of operations that occur on such data. Despite the right choice to designate those entities as responsible for the treatment, it cannot be forgotten that the very sensitive expansion of entities with access to the system, which will take place under the aegis of this diploma, will force reinforced concerns with information security. The stratification of accesses and the guarantee of data integrity must be priority objectives of the

⁴ Concept provided for in Article 4(7) of the GDPR.

Process PAR/2019/39

3

/ NATIONAL COMMISSION -É' ON DATA PROTECTION

responsible, which cannot fail to be linked to the structural reliability of the network that will allow these new accesses.

Therefore, the provision of paragraph 2 of article 11.°5, which states that "Access to information and services available on the technological platform are subject to individual authentication of the user, being established protections based on in access control and user audit files, under the terms of the common user and access management system established by the ACN and

the ACL". essential requirements that make it possible to coherently implement the concerns with access management and user accreditation.

® Personal data processed

Article 15(3) lists the personal data processed⁶ for the purposes of Article 7(2), the latter referring to the national reference model used to ensure the interoperability of the system by all JUL users. Paragraph 4 adds to the aforementioned list of data “the following special categories of data, collected for the purpose of submitting formalities to the authorities and access control: a) Data relating to the health of crew and passengers; b) Biometric data⁷”. These lists of data, although useful and promoting transparency in the use of the data subjects' personal information, do not make it possible to clearly understand who they refer to (which categories of data subjects are affected). The meaning of the collection of videos is unfathomable if the universe of people to whom such collection concerns is not specified, as is the reason for the collection of biometric data of the majority of data subjects subject to appear in the JUL. If paragraph 4 indicates an effort to restrict this universe, one cannot fail to point out that the wording presented does not manage to limit the categories of affected data subjects to the essential. From the outset, the mix of data collection

⁵ Also useful is the wording of paragraph 1 of article 14 regarding the obligation to “The ACN and the ACLs must[r]em guarantee the authenticity of the origin, the integrity of the content and the legibility of the formalities and other information exchanged electronically, from the moment of issuance to the end of the archiving period, implementing auditable controls on the flow of information”.

⁶ These are: Name; Birth date; Naturalness; Nationality; Genre; Type and civil identification number and respective expiration date; Tax Identification Number; Function or professional category; Household; E-mail; Mobile phone contact; Photography and video; Autograph signature and qualified digital signature.

Av. D. CARLOS 1, 134 - lo 1 1200-651 LISBOA | WWW.CNPD.PT | TeL: +351 213 928 400 | FAX: +351 213 976 832

Process PAR/2019/39

3v.

biometrics for “submission of formalities to the authorities and access control” merges into the same group, certainly different categories of holders.

- Rights of data subjects

In turn, paragraph 5 of this same article 15, determines who has access to the personal data contained in the JUL: “a) Any user of the JUL, regarding their personal data; b) The user indicated by each public or private entity, for the purpose of maintaining their entity's access accounts, limited to the data identified in paragraph 3; c) The bodies and services of the State and other legal persons governed by public law, users of the JUL, for the pursuit of their respective powers; d) Any other entities whose interest is justified, with the written consent of the data subjects. Once again, there is a confusion of universes, this time between what is a right of access, within the meaning of article 15 of the GDPR, and what is having access to information of a personal nature by virtue of a specific privilege or credential. . In fact, it would be better to understand if the legislator chose to dedicate an article or a section of the diploma to the subject of processing of personal data, defining there the data to be processed, the prerogatives of action and confidentiality, as well as the security mechanisms, placing in a another article or section on the issue of access definition, here in a more operational logic. When the concepts are mixed up in the same article, the coherence of the legal discipline that is intended to be enshrined is impaired and the certainty regarding the subsidiarily applicable regimes is reduced.

- Confidentiality and retention periods

Finally, and regarding the same mismatch of concepts and regimes, two synthetic notes. The first concerns Article 16, which seems to reserve the guarantees of confidentiality and integrity of information to those classified as commercial or sensitive (cf. Article 16(1) of the draft). However, this compartmentalization of the categories of information that benefit or are eligible for these guarantees puts this regime in clear conflict with the GDPR. Remember that personal data, regardless of their special sensitivity (as provided for in Article 9(1) of the GDPR), deserve similar concerns regarding their security, integrity and confidentiality, as can be seen from a quick reading. of article 32(1) body of the GDPR. And, as mentioned in paragraph 2 of the article just mentioned, there are many times when the risks arise directly from the treatment processes and operations

Process PAR/2019/39

4

M NATIONAL COMMISSION ON DATA PROTECTION

and not merely, as the draft decree-law appears to indicate, of the nature or category of the data processed.

The second note concerns article 19, which governs the matter of data archiving and retention. The confusion of regimes in terms of data protection would find, right in the epigraph, sufficient reasons for critical underlining, since the concept of data

retention refers us to the discipline of conservation of data generated or processed in the context of the provision of communications services electronics⁷, but the main point is different.

As it stands, paragraph 1 of article 19 of the project requires the conservation of data processed in the JUL “for a minimum period of 10 years following the date on which they were collected or on which the execution of sanctions applied in administrative or judicial proceedings and provided that their elimination does not jeopardize the consistency of other data. In turn, paragraph 2 of the same article exempts from this obligation “personal data which are kept for five years after the date of cancellation of the JUL registration and in a historical file for 10 years from the date of their respective elimination in the database. of data.”.

For the CNPD, it is extremely difficult to reconcile these two items. Apparently, the exception in paragraph 2 only operates with respect to data collected for the purpose of registration with the JUL, which strongly limits the specific scope of protection of personal data. In fact, this article can only be interpreted as authorizing the retention of personal data related to the “execution of sanctions applied in administrative or judicial proceedings during such a minimum period of 10 years, which may be exceeded (without any limit foreseen) when its deletion “jeopardizes the consistency of other data. However, the principle of limitation of retention contained in Article 5(1) al. f) of the RGPD, is, in principle, contrary to the existence of unstable or non-closed periods of information conservation, therefore, pointing out a minimum period of 10 years, especially when data categories related to criminal convictions and administrative offences are concerned, it indicates, from the outset, excessive⁸, and projects an indeterminability that is inconsistent with the current data protection regime. And the more incoherent it becomes when it makes it depend

⁷ Law No. 32/2008, of July 17

⁸ With the risk of taking an ancillary sanction, which may even exceed any legal deadlines that may be invoked regarding the recidivism or prescription of proceedings.

AV. D. CARLOS I, 134 - 1o | 1200-651 LISBON | WWW.CNPD.PT | TeL: +351 213 928 400 | FAX: +351 213 976 832

Process PAR/2019/39

4v.

the elimination of such data in the absence of a risk to the consistency of other data.

In short, it will be advisable to rethink this entire article and adapt its future wording to data protection legislation.

C. Need for an Impact Assessment on Data Protection As is evident from the object of this draft decree-law, in the future we will have a reinforced centralization of information coming from several and different actors in the transport of people and goods sector. This concentration of information, also of a personal nature, generates greater risks when considering the potential dangers facing personal databases at the present time.

Bearing in mind the different purposes allowed by the technological platform that implements the JUL, which includes border controls regarding the movement of persons (Article 9(2)(c)), information on transported persons (Article 9, n.º 2, paragraph k) and Border controls and access of persons to premises (Article 9, paragraph 2, paragraph l)), it is easy to understand the extent of the treatments at issue here. Additionally, it is certain that a superlative amount of personal data concerning an immeasurable number of people is registered, to which a large number of potential natural and legal persons with access to the JUL are linked, with the additional risk of processing categories data (biometric and health data), the CNPD considers that a Data Protection Impact Assessment should be seriously considered, as set out in article 35 of the GDPR, prior to the implementation of the JUL.

In this regard, paragraph 3 of the aforementioned GDPR article mentions the obligation to carry out impact assessments whenever there is: “a) Systematic and complete assessment of personal aspects related to natural persons, based on automated processing, including the definition of profiles, on the basis of which decisions are adopted that produce legal effects relative to the natural person or that significantly affect him in a similar way; b) Large-scale processing operations of special categories of data referred to in Article 9(1) or personal data relating to criminal convictions and offenses referred to in Article

Process PAR/2019/39 5

,

/ ,

NATIONAL COMMISSION

L OF DATA PROTECTION

In view of the quantity and quality of data, the profusion of actors on the platform and the legitimate interpretation that links the Janela Única Logística to a system with the ideal technical characteristics to fit into both paragraphs of article 35, paragraph 3 of the GDPR9, it is seriously advisable to carry out such a prior assessment.

III. conclusions

This draft decree-law represents an ambitious step in terms of the convergence of databases, especially in terms of interoperability, noting some notes of careful and consistent concern with matters of personal data protection. Even so, the CNPD warns of the need to:

The. Clarify the existence of JUL's interconnections with other databases, making them positive in the text of the diploma and properly determining their regulation, with the CNPD being called upon to comment on this regulation;

B. Highlight the issues of protection of personal data from those related to the management of information that is purged from said data, enhancing the clarity of the rules specifically applicable to the different areas that are in focus, especially regarding the realization of the rights of data subjects and respect for the structuring principles of data protection;

ç. Consider carrying out an impact assessment on data protection prior to the operation of the Single Logistics Window, in order to anticipate, manage and, if possible, eliminate the potential risks to the rights and freedoms of individuals linked to the concentration of information from personal nature, as well as the multiple and different accesses that are now made possible by this platform.

Lisbon, July 16, 2019

Filipa Calvão (President)

9 And without prejudice to the possibility of including the treatments provided for in one of the situations in which the impact assessment on data protection is mandatory, listed in the list approved by the CNPD and published in Regulation No. 1/2018, available at https://www.cnpd.pt/bin/decisoos/regulamentos/regulamento_1_2018.pdf.

Av. D. CARLOS I, 134 - 1o | 1200-651 LISBON | WWW.CNPD.pt | TEL: +351 213 928 400 | FAX: +351 213 976 832