NATIONAL COMMISSION

, DATA PROTECTION

OPINION No. 4/2018

I. Order

The Chief of Staff of the Assistant Secretary of State and Finance sent the National Data Protection Commission (CNPD), for an opinion, the draft Law Proposal transposing Directive (EU) 2015/2366 of the European Parliament and of the Council, of 25 November 2015 on payment services in the internal market. The draft diploma regulates, in the annex, the Legal Regime for Payment Services and Electronic Money and also implements, in the domestic legal order, Regulation (EC) no. (EC) No. 260/2012, of March 14, and Regulation (EU) 2015/751, of April 29, 2015.

The request made stems from the powers conferred on the CNPD by paragraph 2 of article 22 of Law no. 67/98, of 26 October, amended by Law no. Protection of Personal Data (hereinafter, LPDP) -, and the opinion is issued using the competence set out in paragraph a) of paragraph 1 of article 23 of the same legal diploma, being restricted to aspects related to data protection personal.

II. appreciation

1. Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market (Directive PSD2), which is intended to be transposed, aims to encourage the development of the use of electronic payments and ensure they are made securely. To achieve this objective, rules that reinforce transparency are established, among others. However, in order to ensure this transparency, it is important that it is clear that the provision of payment services, when relating to individuals, involves the processing of personal data.

It is on this assumption that Recital 89 of the PSD2 Directive indicates that the data protection regime applies to the processing of personal data and, in

Useful □as from 10 am to 1 pm

doubts@cnpd.pt

Case No. 976//2018

two

(r

In particular, it states that the exact objective must be specified, the applicable legal basis must be mentioned, the applicable safety requirements laid down in Directive 95/46/EC must be met and the principles of necessity, proportionality, limitation of purpose and period of data retention provided. Likewise, data protection by design and data protection by default should be incorporated in all data processing systems developed and used within the framework of this Directive.

Thus, it is noted that although Subsection IV of Section III of Chapter III of Title III of the Annex to the Draft Law contains an article on data protection1, article 136, the truth is that it does not refer directly to for the legal regime for the protection of personal data, nor does it regulate all the aspects that are required for the respect of this fundamental right. In this way, it is either chosen to regulate the rules to which it is subject in each article in which operations are foreseen, or, in a situation that seems more appropriate, the rule on personal protection is used for that purpose. define all the elements that that regime requires.

2. Also as a general note, it is noted that the references made in Directive PSD2 to Directive 95/46/EC, of 24 October, on the protection of individuals with regard to the processing of personal data and the free movement of such data , should take into account that this will be replaced by Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and free movement of this data (General Regulation on Data Protection - RGPD), which has been in force since May 25, 2016 and will apply from May 25, 2018, revoking Directive 95/46/EC. Now, since the GDPR creates new

1 The title of which, for reasons of clarity, should be, either in the Subsection or in the article itself, Protection of Personal Data.

obligations for those responsible for data processing2, namely regarding the elements of the right to information and obtaining consent, and new rights of the holders of personal data, it is desirable that the proposal already takes into account all the changes imposed by the RGPD.

3. In this sense, relating the new obligations of those responsible for processing personal data to the requirements of this proposal, it is noted that article 19(2)(o) provides that one of the elements that must accompany the request authorization to establish themselves as payment or e-money issuing institutions is the security policy document. In this standard, it is mandatory that a detailed assessment of the risks be carried out and the description of the measures taken to protect users against these risks, highlighting, in particular, fraud and the illicit use of sensitive and personal data.

The assessment provided for here coincides with the obligation to carry out an impact study on data protection (cf. Article 35 of the GDPR), which is an indispensable instrument for determining the security mechanisms and measures to be adopted in order to mitigate the risks that the processing of personal data entails. For reasons of terminological consistency, the expression sensitive and personal data should be corrected, as sensitive data are also personal data (cf. point a) of article 3 and article 7 of the LPDP).

4. Chapter VII of Title II, on supervision, provides3 in article 61 for cooperation between Banco de Portugal, as a supervisory authority, with other competent authorities under Union law or national law applicable to payment service providers and electronic money institutions (paragraph 1). In addition to this obligation of cooperation, paragraph 2 provides, in subparagraphs a) to d), for the exchange of information with these entities. The novelty, in relation to the directive,

2 By way of example, the following service providers are mentioned, which, for the operations they carry out, assume the quality of responsible for the processing of personal data (cf. subparagraph d) of article 3 of the LPDP and paragraph 7 of article 4 .° of the GDPR), provider of account information services,

payment initiation service provider, payment service provider.

3 Em4transpositionQ-of-article-2S^-of..PSD2__ Directive

introduced by the national legislator in paragraph c) is, if we read the rule correctly, the provision for the exchange of information with the CNPD in the context of the processing of personal data. Indeed, if one understands the need for cooperation between these two supervisory authorities within the scope of the legislation that is being transposed, the graft of the exchange of information with the CNPD, in a norm that in its origin seems to have in view the exchange of information between competent authorities only in matters of money laundering and terrorist financing4.

5. Article 71 regulates the communication of security incidents. However, the obligation to notify security breaches in the context of the protection of personal data is regulated in Article 33 of the GDPR and is not, and could not be, excluded by that directive. In this way, for reasons of legal clarity, it is convenient to note in this rule the duty of communication to the CNPD, which in any case falls on those responsible for the processing of personal data.

With regard to the possible notification by Banco de Portugal to the relevant national authorities, it is important to emphasize that more important than this notification, in the context of data protection, would be the forecast of the need for conciliation between Banco de Portugal and the CNPD, in order to safeguard the various rights and interests involved (e.g. the right of data subjects to know about the violation of their personal data and the public interest in preventing risks to the financial system).

6. Also for reasons of legal clarity, in Chapter II, on transparency and information requirements relating to payment services, it will be appropriate that the duty of information provided for in article 10 of the LPDP and in articles 12 and ss. GDPR It should be noted that, despite the provisions of paragraph 2 of article 79 of the proposal, no fees can be charged for providing information provided for in the aforementioned data protection rules.

4 Other relevant authorities designated pursuant to this Directive, Directive (EU) 2015/849, as well as other Union law applicable to payment service providers, such as applicable legislation on money laundering and terrorism -cf. Article 26(c) of the PSD2 Directive.

/ NATIONAL COMMISSION

, DATA PROTECTION

ill. conclusions

From the above, it follows that data protection obligations must be specified through concrete safeguards applicable to all situations in which the processing of personal data is foreseen, making it clear that the provision of payment services implies the processing of personal data and, to that extent, the obligations arising from the legal data protection regime will have to be fulfilled. Thus, Article 136 must make a direct reference to this regime, regulating all the aspects that are required for the respect of this fundamental right.

A substantive provision should be added which, embodying recital 89, provides that data protection by design and data protection by default, provided for in Article 25 of the GDPR, must be incorporated in all data processing systems. data developed and used in the framework of payment services and electronic money.

This is the opinion of the CNPD.

Lisbon, January 31, 2018

Filipa Calvão (President who reported)

Rua de São Bento, 148-3° Tel: 213 928 400

1200-821 LISBON Fax: 213 976832

www.cnpd.pt

PRIVACY LINE

Weekdays from 10 am to 1 pm

doubts@cnpd.pt