□I

Process PRE/2020/1 | 1 f~

NATIONAL COMMISSION

DATA PROTECTION

RESOLUTION/2020/238

I. ORDER

Hospital de Braga, E.P.E. (hereinafter, Hospital), submitted to prior consultation of the National Data Protection Commission (hereinafter, CNPD) the processing of personal data resulting from the statistical processing of data on purchases and consumption of medicines within the scope of hospital activity, for use in the Hospital Study National published by IQVIA Solutions Portugal, Lda. (hereinafter, IQVIA). It did so under paragraph 1 of article 36 of Regulation (EU) 2016/679, of 27 April 2016 - General Regulation on Data Protection (hereinafter, GDPR), after having carried out the assessment of impact on data protection and following the opinion of the respective data protection officer.

This determination is issued within the scope of the CNPD's powers and competences as an independent administrative authority with powers of authority to control the processing of personal data, conferred by subparagraph 0 of paragraph 1 of article 57, in conjunction with subparagraph a) of paragraph 3 of article 58, and with paragraph 2 of article 36, all of Regulation (EU) 2016/679, of 27 April 2016 - General Regulation on Data Protection (hereinafter, RGPD), in conjunction with the provisions of article 3, paragraph 2 of article 4, and paragraph 2 of article 6, all of Law No. 58/2019, of August 8, which enforces the GDPR in the domestic legal order.

II. ASSESSMENT

The prior consultation arises in the context of the conclusion, between the Hospital and IQVIA, of a co-responsibility agreement in the provision of data regarding purchases and consumption of medicines carried out within the scope of the Hospital's care activity.

Within the scope of the aforementioned agreement, a “purchase file” and a “consumption file” will be sent monthly from the Hospital to IQVIA. The «purchase file» includes information on all purchases made from suppliers, as well as any returns, and involves the following set of data: supplier code, name of

supplier, product registration code1, product code, product name, description of the “form”2, hospital unit, units, value and price3. The «consumption file» refers to «all supplies and eventual returns in the different services/cost centers in the hospitab and contains the following information: «cost center code, cost center name, product code, name of the product, description of the form, hospital unit, diagnosis code, name of diagnosis, fictitious code of the user4, gender of the user, date of birth of the user, units, value and price'.

It is also noted that the information to be communicated monthly to IQVIA is extracted from the Hospital's database by Glintt Healthcare (GLINTT), a data processing subcontractor, which, after the extraction and before the transfer of the data to IQVIA, proceeds encoding the user's identification - proceeds, as described in the application, to "pseudonymize the user ID".

The main question posed in the request for prior consultation relates to the nature of the information processed by IQVIA: whether the data at issue are pseudonymised and, to that extent, also personal data, as such their treatment is subject to the RGPD, or if, at the otherwise, they correspond to anonymized data.

According to the documentation that accompanies the consultation request, IQVIA claims that there is no processing of personal data, because it does not know the encryption key for the user's identification, so the information is, for it, non-identifiable.

On the contrary, within the scope of the impact assessment carried out by the Hospital, it is argued that, in addition to the data being pseudonymised, "they still carry a set of data that can make people identifiable (date of birth, diagnosis codes, dates of consumption, prescribing service)', concluding that there is a very high risk if the recommended mitigating measures are not adopted, having

1 Product registration number at Infarmed, followed by a hyphen and the description "Name - Farm Form. -Dosage" present in Infarmed's National Hospital Drug Code (CHNM) file. Example: "9403626-Flemeran Gel - Gol -10 mg/g' or 'OOOOOOOO-Olbetam* - Capsule - 250 mg"

2 Example: unit, tube, gram, capsule, vial.

4 Example of a purchase file record: 123;”Supplier A”;”9403626-Flemeran Gel - Gel - 10 mg/g";10015470;”Fleparinoid 10 mg/g

Bisn Gel 40 g";"EPISE";" Center!";20000;10620000;531000.

4 According to IQVIA's documentation, "(n)with regard to this code, it results from an anonymization operation carried out by Hospital de Braga, which creates and has access to the encryption key, which is not the same, in any case communicated to IQVIA'.

i

NATIONAL COMMISSION

DATA PROTECTION

account that they involve special data categories and that the processing is on a large scale.

Let's see.

The information from the Hospital's database that is extracted to be made available to IQVIA using software that encrypts the Hospital's user's internal code, so that, from the outset, IQVIA does not know the identity of the data subject object of communication. . In this sense, IQVIA could today only claim that the data are pseudonymized for it, according to the concept now presented in the GDPR (Article 4.75).

In fact, under Directive 95/46/EC and Law no. that it could be said that the encrypted data made available to another entity were not, for that entity, personal data when it was not possible, or only with a very high effort, to re-identify the natural persons whom they respect. The technological evolution that took place in the meantime, even during the validity period of those diplomas, and in particular the generalization of the use of certain Artificial Intelligence technologies, changed the degree of difficulty of the coding reversal processes, enhancing the reasonable probability of their occurrence, making European legislation today qualify that information, whenever it can be attributed to a natural person through the use of supplementary information, such as personal data5.

Indeed, the GDPR formalized the concept of pseudonymization, as opposed to anonymization, to characterize the operation on personal data that makes the data subject unidentifiable without resorting to supplementary information, provided that such information is kept separately and technical and organizational measures

5 To what the Working Group of Art. 29, in its opinions no. 4/2007, p. 16, available at

https://ec.europa.eu/iustice/article-29/documentation/opinion-

recommendation/files/2007/wpl36 en.pdf, and No. 5/2014 (WP216), p. 9, available at

https://ec.europa.eu/iustice/article-29/documentation/opinion-recommendation/files/2014/wp216 en.pdf, highlighting that the risk of identification can increase over time and that it also depends on the development of information and communication technologies.

to ensure that personal data cannot be attributed to an identified or identifiable natural person, specifying, in recital 26 of the GDPR, that pseudonymised data are still personal data, for the purposes of applying the personal data protection regime and the obligations imposed on controllers and processors.

Precisely, in the specific case, it is important to consider the set of pseudonymized information that is extracted to make available to IQVIA, in order to understand whether or not, through its relationship with other information, there is a reasonable probability of re-identifying the data subjects. What must be done, as specified in the GDPR (recital 26) and had been stated by the jurisprudence of the Court of Justice of the European Union6, as well as by the Art. 29, taking into account all objective factors, such as costs and the time required for identification, taking into account the technology available at the time of data processing and technological developments.

In fact, the technological developments that have taken place in the last decade have made it possible to identify more expeditious ways of attacking systems and operations such as encryption, hashing, or data encryption. In the field of cryptography, for example, there were algorithms that were considered obsolete in the last decade (e.g., MD5 and SHA-1).

All this to reinforce what is underlined in the opinion of the Data Protection Officer of the Hospital: the 2010 CNPD letter, which stated that there was no probable risk of re-identification of data subjects in the procedure followed by IMS Health7 cannot be taken as crystallized in time and cover, almost ten years later, the processing of information, excluding it from the personal data protection regime, without analyzing and considering the exact terms in which it is carried out today by IQVIA, in the light of technology available and the risks to which it is currently subject. All the more so as the information on the health of users is

at stake, which is subject to a specially reinforced regime of protection in the RGPD.

Therefore, it is important to consider, from the outset, the set of information communicated to IQVIA and which may facilitate the re-identification of the data subject, namely: date of birth (year/month/day), sex, disease diagnosis code (and name of

6 Cf. Judgment Patrick Breyer v. Federal Republic of Germany of 19 October 2016 (C-582/14), § §

41 to 46.

7 IQVIA SOLUTIONS PORTUGAL, LDA is the new name of IMS HEALTH, LDA. in Portugal, since the amendment of the articles of association of 02/28/2018.

diagnosis), specialty of the prescribing physician, drug code, date of consumption (year and month). However, considering that today the probability of re-identification of the data subject presents itself with a degree of reasonableness when three categories of data are available, it is considerably accentuated if we add to this obvious factors or attributes, such as the diagnosis of a rare disease.

In addition, the CNPD does not have information on the pseudonymization process carried out by GLINTT, since the Hospital de Braga itself points out that “the process of encrypting the patient's code is not known”. As a result, it is not possible to determine whether the applied pseudonymization makes the process of association with the respective holder sufficiently difficult. Furthermore, the lack of information on this process also does not make it possible to know if it is possible to relate identifiers from different months, that is, if the algorithm applied by GLINTT produces different codes in different months for the same user numbers. If the resulting codes remain unchanged for each user, it is possible for IQVIA to perform a profile of the patient's evolution (e.g., reduction or increase in drug doses), which translates into a serious risk for the privacy of the holders.

In fact, it should be noted that the risk of identifying data subjects is not restricted to hospital users, but also extends to prescribing physicians, namely in situations where a drug is used in an introductory way.

In short, it is not only the processing of personal data carried out by the Hospital (data availability), but also the treatment carried out by IQVIA on the information it receives from the Hospital that constitutes a processing of personal data, which fall

into the category of data special or sensitive, provided for in Article 9(1) of the GDPR, and, although the data are pseudonymised, their processing, in the terms and with the scope and regularity with which it is carried out, still presents a high risk for the privacy of data subjects. This is why it is justified to carry out an impact assessment on the protection of personal data by IQVIA, which guarantees the mitigation of risk, in accordance with Article 35(1) and (3)(b) of the GDPR and CNPD Regulation No. 798/2018, of 30 November.

III. CONCLUSION

In short, the CNPD understands that the processing of personal data subject to this prior consultation does not provide for sufficient measures to guarantee the privacy of the data subjects and

that those responsible for the treatment - therefore, Hospital de Braga, E.P.E., and IQVIA Solutions Portugal, Lda. - should seek to identify additional measures to limit, as far as possible, the risk to data subjects.

This may include, in particular, ensuring that the information is extracted with lower re-identification factors - e.g., omitting the day (and month, when not relevant) of birth or indicating age ranges; omit pathologies that, due to their atypical nature, facilitate re-identification.

1. Therefore, under Article 36(2) and Article 58(3)(a) of the GDPR, the CNPD recommends that those responsible find ways to reduce, as much as possible, the probability of identification of data subjects, highlighting here the adoption of appropriate measures to ensure that:

1. The pseudonymization process applied by Glintt Healthcare produces different results for the same number of users, to reduce the probability of correlation of data from different months;

ii. Transmission of files by file transfer protocol! (FTP) between Hospital de Braga, E.P.E., and IQVIA Solutions Portugal, Lda., is done over a secure channel (e.g., TLS or equivalent), since the FTP service does not guarantee the confidentiality of communications.

2. Also under Article 36(2) and Article 58(2)(f) of the GDPR, the CNPD determines that the subcontracting entity does not

extract the data until it receives an indication of the controller that appropriate additional measures have been taken to mitigate the risks to the rights of data subjects.

Lisbon, May 21, 2020

Filipa Calvão (President)