Processing personal health data for insurance purposes under GDPR

15 October 2019 | Contributed by Morais Leitão, Galvão Teles, Soares da Silva & Associados

AUTHOR

Helena Tapp Barroso

Legitimate basis for data processing
GDPR Data Protection Act and health data for insurance purposes

Although the government published an implementation bill to transpose the General Data Protection Regulation (GDPR) into domestic legislation in March 2018, the approval and publication of the law took over one year (for further details please see "Legal basis for processing personal health data for insurance purposes"). On 8 August 2019 the Portuguese GDPR Data Protection Act was finally published, becoming fully effective the day after publication.

Legitimate basis for data processing

One of the key issues that the Portuguese insurance industry faced in 2018 was the legitimate basis for insurers to process (and continue processing) health data required for the performance of insurance contracts – in particular, health, personal injury and life insurance contracts. At that time, all attention was focused on the possibility of (and desire for) the GDPR Data Protection Act to provide specific grounds for the processing of health data for insurance reasons. This could have been achieved by including legal provisions in the implementation law that:

- acknowledged a "substantial public interest" pursuant to Article 9(2)(g) of the GDPR for the processing of special categories of data necessary for insurance purposes;
- respected the requirements of proportionality sought by the legislature;
- respected individuals' right to data protection; and
- provided for suitable and specific measures to safeguard data subjects' fundamental rights and interests.

The GDPR Data Protection Act would thus have been in line with GDPR implementation laws passed in a number of other EU member states (eg, the United Kingdom, Ireland and Spain), which contain derogations for the processing of health data for insurance purposes based on the recognition that such processing is required for reasons of substantial public interest (Article 9(2)(g) of the GDPR).

Alternatively, this could have been achieved by mirroring the relevant legal provisions granted to EU member states by Article 9(4) of the GDPR to maintain or introduce "further conditions... with regard to the processing of genetic data, biometric data or data concerning health" in line with an interpretation consistent with Recital 10 of the GDPR, which acknowledges a "margin of manoeuvre for Member States to specify rules, including for the processing of special categories of personal data ('sensitive data')". This includes personal health data, and Recital 10 provides EU member states with the possibility to determine "more precisely the conditions under which the processing of personal data is lawful".

The draft GDPR Data Protection Act included no provisions on this subject. Following consultation on the draft proposal, the supervisory authority underlined the relevance of the issue and recommended that such a derogation should be included in the final version of the law.

GDPR Data Protection Act and health data for insurance purposes

Compulsory insurance versus voluntary insurance coverage

The final wording of the GDPR Data Protection Act was approved without any exemptions or provisions regarding the legitimate basis on which insurers can process health data (or any other special category of data) for insurance purposes.

Where does this leave insurers? Essentially, where they were on 25 May 2018, but not exactly. Based on the opinions of legal scholars, it is now clear that for compulsory insurance (be it first-party or third-party insurance), the processing of health data required for the execution and performance of

an insurance contract can be based on a substantial public interest pursuant to the exemption provided for in Article 9(2)(g) of the GDPR, even though the GDPR Data Protection Act does not explicitly provide for this exemption.

Under Portuguese law, insurance coverage for professional liability and liability arising from specific activities is compulsory. In a total of 115 recent insurance cases, there were 36 examples of compulsory insurance for personal accident, health and life-related insurance claims.

There are different reasons why compulsory insurance is required that will not apply to all cases or classes of insurance. However, it is reasonable to argue that public interest concerns are the basis of EU member states defining the risks for which insurance is compulsory and providing for that in legislation. Based on the Data Protection Authority's written opinion on the draft GDPR Data Protection Act, this understanding has been accepted and adopted by insurers in Portugal.

In the specific case of compulsory insurance for workplace accidents, the grounds for processing health data are covered by Article 9(2)(b) (ie, data processing "necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of... social protection law").

Insurers must now revisit their position on the legitimate grounds for processing health data with regard to voluntary coverage. The most critical cases are voluntary health and life insurance and all voluntary insurance covering personal injury risk. This is particularly relevant to life insurance considering that the GDPR Data Protection Act (pursuant to Recital 27 of the GDPR) provides that the processing of certain categories of personal data of deceased persons is subject to the rules and principles of the GDPR (ie, personal data included in the special categories mentioned in Article 9(1) of the GDPR, including health data, private data and images and personal data in communications).

Insurers should thus check their explicit consent provisions for the processing of personal health data tied to insurance contracts and whether they comply with the freedom of consent principle. While it is impossible to sustain that such insurance contracts and coverage can be executed without the processing of health data, the contract law parameters set out in Article 6(1)(b) of the GDPR are not (on a standalone basis) a legitimate basis for processing health data or any other special category of data subject to Article 9 of the GDPR.

The nature of the risks covered should make it clear that the fact that an insurance contract is tied to consent does not imply that consent is not freely given. Article 7(4) of the GDPR does not exclude the possibility of the explicit consent exemption applying to the processing of certain categories of data required for the performance of the contract in question:

> *when assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data* ***that is not necessary for the performance of that contract****.* (Emphasis added.)

In its Guidelines on Consent under the GDPR (revised and adopted on 10 April 2018), the Article 29 Data Protection Working Party stated as follows:

> *Article 7(4) GDPR indicates that, inter alia, the situation of "bundling" consent with acceptance of terms or conditions, or "tying" the provision of a contract or a service to a request for consent to process personal data* ***that are not necessary for the performance of that contract or service****, is considered highly undesirable. If consent is given in this situation, it is presumed to be not freely given (recital 43)... The two lawful bases for the lawful processing of personal data, i.e. consent and contract cannot be merged and blurred... and additionally that] according to Opinion 06/2014 of WP29, the term "necessary for the performance of a contract" needs to be interpreted strictly.... There needs to be a direct and objective link between the processing of the data and the purpose of the execution of the contract.* (Emphasis added.)

The guidelines also state that "if a controller seeks to process personal data that are in fact necessary for the performance of a contract, then consent is not the appropriate lawful basis" and that the appropriate lawful basis "could then be Article 6(1)(b) (contract)". However, this is not the case when it comes to health data or other special categories of data, as the appropriate lawful basis of Article 6 of the GDPR does not apply or must at least be combined with Article 9's exemptions.

The Article 29 Data Protection Working Party acknowledges this point in its guidelines, which state as follows:

> *Article 9(2) does not recognize "necessary for the performance of a contract" as an exception to the general prohibition to process special categories of data. Therefore*

controllers and Member States that deal with this situation should explore the specific exceptions in Article 9(2) subparagraphs (b) to (j). Should none of the exceptions (b) to (j) apply, obtaining explicit consent in accordance with the conditions for valid consent in the GDPR remains the only possible lawful exception to process such data.

However, it seems likely that – notwithstanding the restrictions established based on the interpretation of Recital 54 of the GDPR – the specific exemptions set out in Article 9(2)(b), (g), (h) and (i) of the GDPR will be seen in future to provide a legitimate basis for the processing of health data required for certain insurance contracts, including health insurance contracts..(1)

For further information on this topic please contact Helena Tapp Barroso at Morais Leitão Galvão Teles Soares da Silva & Associados by telephone (+351 21 381 74 00) or email (htb@mlgts.pt). The Morais Leitão Galvão Teles Soares da Silva & Associados website can be accessed at www.mlgts.pt.

Endnotes

(1) Recital 54 states as follows:

> *The processing of special categories of personal data may be necessary for reasons of public interest in the areas of public health without consent of the data subject... [and that] In that context, 'public health' should be interpreted as defined in Regulation (EC) No 1338/2008 of the European Parliament and of the Council (1), namely all elements related to health, namely health status... the determinants having an effect on that health status, health care needs, resources allocated to health care, the provision of... as well as health care expenditure and financing, and the causes of mortality... [but also that] such processing of data concerning health for reasons of public interest should not result in personal data being processed for other purposes by third parties such as employers or insurance and banking companies.*
