VOICU FILIPESCU
Attorneys at Law
News in Laws – Legal Monthly Newsletter
November 2018

cover article

GDPR's Impact on Healthcare Services

by Vlad Irimia, Senior Associate Voicu & Filipescu

Once it is accepted that Regulation 2016/679 on data protection[1] (hereafter referred to as the "**Regulation**" or "**GDPR**") is fully applicable not only to the various legal entities (including small companies with a rather reduced level of activity), but also in the case of individuals processing personal data, during their activity, the specific implications of the Regulation on healthcare activities can be raised.

In this context, alignment with GDPR requirements implies a detailed analysis of the particularities of the medical field, especially taking into account the legal provisions applicable in this field (including the specific legislation regulating the profession of physician) in order to respond to the aims of the Regulation.

Specific aspects

In addition to the general need to comply with GDPR provisions - issues that are not negligible, however, taking into account the various relevant issues in the context of an analysis (such as: activity level, specific information flows, type and level of relationships with others, belonging to a group of companies or complex operations with an impact on the processed personal data) - the specific nature of the medical field can bring additional implications that need to be addressed from a data protection perspective in the particular context of a regulated activity and where a significant part of the information represents special categories of personal data, in the GDPR sense.

At first glance, it may be concluded that, at the level of a medical practice, the requirements of the Regulation can be more easily implemented and observed during their application; one main argument could be that the current activity in a simple medical practice involves a less complicated flow and level of information, and the main GDPR compliance issues can be easily identified.

Depending on the specific way of organizing the practice, in accordance with the legal provisions, and taking into account the relationships established by the medical practice with its various partners - relationships that include specific service providers (*e.g.* IT service providers, accounting / payroll services providers) as well as collaborations with other practices or companies / clinics operating in the medical field - a number of rather complex issues that may make compliance with Regulation more difficult could arise.

1 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 on the free movement of such data, repealing Directive 95/46/EC

Potential difficulty aspects

Among others, the following specific matters might involve difficulties in analysis:

(a) Identifying relationships with partners

In addition to correct identification of all processed personal data, implementation of minimum protection measures, drafting and providing the data subjects with the necessary information under GDPR, or ensuring conditions for them to exercise their specific rights, in practice, it may prove quite difficult to analyze the relationships established with different contractors, from the perspective of the Regulation.

Since the identification of a *controller - controller*, *controller - processor* or *joint controllers* relationship may impose a number of specific obligations (in accordance with the Regulation), both the agreed contractual circumstances and the reality of the relationship between the parties will be essential in order to determine the specific steps for ensuring protection of personal data.

Under these circumstances, the specific guidelines adopted by the former *Article 29 Working Party* on *controller* and *processor* concepts may prove extremely useful in the assessments to be made in this respect, on a case-by-case basis.

In addition, where available, various instructions, guidelines or other similar guidance adopted by professional associations, professional regulatory bodies and/or other bodies active in the healthcare field, should be taken into account, for the sake of clarity.

(b) Identifying specific obligations depending on the processing circumstances

Another potential issue that should be addressed appropriately derives from the specific scope of data processed in the medical field.

In particular, the principle of data minimization under the GDPR must be circumscribed in the context of the medical activity, since certain data that, at first sight, could be considered excessive, may be of particular relevance and its processing is necessary for the purpose of conducting medical consultations and prescribing specific recommendations / treatments (such as: information on eating habits or related to work or other personal issues).

Therefore, the information processing framework should be analyzed in detail, on a case-by-case basis, taking into account both the wider context of the medical service provided to the data subject and the need to process certain categories of data that can be of particular relevance together with various other elements relating to the data subject.

(c) Identifying the specific basis for data processing

This issue may also raise certain difficulties in the specific context of the processing of special patient data categories.

In particular, the specific requirements of the Regulation have a significant impact on the processing operations, bearing in mind that, historically, processing of patient data has in most cases been carried out on the basis of their implicit consent, but this aspect should be analyzed (and even reconsidered) from the GDPR perspective.

The basis for the processing of special categories of data will have to be identified both by reference to the provisions of art. 6 GDPR as well as by reference to the provisions of art. 9 GDPR, taking into account, *inter alia*, the purpose of the processing (which facilitates the correct identification of the basis of the processing operation).

Additionally, in the context of identifying the basis of processing, one should also consider and separately address the specific requirements under medical legislation and data protection rules, each with their own regulatory scope.

By way of example, there may be cases in which personal data is processed on the basis of legal requirements or legitimate interests, while also being necessary in the context of occupational healthcare requirements; at the same time, however, from medical legislation perspective, the medical service (and, implicitly, the data processing) can be performed on the basis of the patient's informed consent (which is different, with respect to content and purpose, from the consent for processing under the GDPR).

(d) The need to conduct a data protection impact assessment

Last but not least, the data protection impact assessment (DPIA) is also a sensitive query that should be considered in the specific context of the activity being carried out.

This issue should have to be dealt with on the basis of the specific requirements of the Regulation (including by reference to the relevant recitals in the GDPR preamble) and taking into account the mandatory cases defined at national level for carrying out such an impact assessment (as detailed in the content of ANSPDCP[2] Decision No 17/2018).

Particularly relevant is the situation of large-scale processing of patients' genetic and/or health data, or the large-scale processing of employee's data (through automatic monitoring and/or systematic recording of behavior) where an appropriate impact assessment is required. Generally speaking, the key issue in these cases is the manner of interpretation and application of the concept of *large scale*, a matter that might prove even more problematic in the case of a simple medical practice than that of a private health clinic.

2 ANSPDCP is the National Personal Data Processing Supervising Authority.

Conclusions

The very diverse nature of the personal data which is typically processed by healthcare professionals, the specific regulations in this field as well as the particular context of relationships established with both the data subjects and the various persons involved in the data processing activities need to be analyzed in detail, to properly identify and address the implications of these operations, in the light of the requirements of the Regulation, as well as according to the realities of the medical activity.

Any materials prepared by various professional associations, regulatory bodies and/or other bodies active in the medical field may prove extremely useful in defining, at least in principle, certain recommendations to be followed by those acting in this field. Indicatively, one can take into account materials prepared by national authorities in the field of personal data protection or various guidelines prepared at the level of professional associations / bodies from other EU Member States, which may provide useful recommendations in the context of compliance with GDPR requirements.