WilhelmGilliéron
AVOCATS

Auteur: Wilhelm Gilliéron Avocats | Le : 4 October 2021

Data protection and the liberal professions: not so complicated

On 10 June 2021, the Italian data protection authority fined a dentist € 20,000 on the grounds that the dentist had refused to treat a patient with the HIV virus without having clearly stated that such disclosure could lead to a refusal of treatment, and not only to consequences as to the possible treatment.

While this is a special case, it cuts short any belief that data protection compliance only concerns large companies, the only ones able to exploit personal data on a massive scale and therefore the only ones to be in the crosshairs of the authorities and possible sanctions.

The question then arises as to what measures doctors, dentists and other lawyers (whom I will then refer to as “practitioners” for the sake of simplicity) should reasonably implement to avoid any misadventure.

A. ***No application of the GDPR***

In reality, these steps are quite simple. First of all, it should be remembered that, unless practitioners deliberately target European residents, they should not be submitted to the GDPR, but only to the Federal Data Protection Act, a revision of which is expected to come into force during 2022.

2. ***Legal obligations***

Without going into detail, practitioners are at first sight subject to three obligations, the scope of the first two of which should however be put into perspective:

1. **The register of processing activities**

The obligation for practitioners to keep a register of processing activities requires in principle to determine, among other things, the type of processing, the purpose of the processing, the categories of persons (patients, employees, sometimes suppliers) and the categories of personal data (which may be sensitive in the medical field) processed, as well as the possible transfers abroad and the recipients of these possible transfers.

However, the Federal Council has exempted companies with fewer than 250 employees from this obligation if the processing concerned does not involve the processing of sensitive data on a large scale or does not lead to the establishment of high-risk profiling. While high-risk profiling may not be possible for practitioners, the processing of sensitive data is certainly possible, particularly in the medical field. However, the “large-scale” requirement seems to presuppose massive processing within a hospital or clinic, which, at first glance, should not be the case for a private practice.

This is an obligation that practitioners should be exempt from.

2. **The duty to inform**

All data controllers, including practitioners, are in principle obliged to inform the data subject adequately about the collection of personal data and the purpose of the collection (in concrete terms, it is necessary to explain what will be done with the data and why it is necessary to collect it).

While such an obligation is easy to implement, the law provides that when the controller is a private person subject to a legal obligation to maintain secrecy, he or she is released from this obligation. Practitioners are subject to such an obligation by virtue of Article 321 of the Criminal Code; it must therefore be concluded that they have no legal obligation to inform their patients or clients of the processing carried out.

There is, however, an exception to this principle. When the processing contemplated requires the processing of sensitive data, such as medical data, the express consent of the data subject is then required, which implies that the latter must be duly informed of the processing concerned in order for his or her consent to be validly given, it being specified that in Swiss law, unlike European law, consent is considered to be express even if it is given by reference to general conditions.

3. **Adequate security measures**

In the end, it is really the obligations on practitioners to ensure that adequate security measures have been put in place to protect data against the risks involved that are most important.

From this point on, what advice can one give to practitioners?

3. ***Practical considerations***

1. **On the technical side**

Three points:

- Firstly, the fact that the practitioner must ensure that his infrastructure guarantees a form of security for his patients' or clients' data. In this respect, it should be noted that it is now widely accepted that the use of a **cloud provider** is admissible insofar as the latter appears to be an auxiliary (in the same way as the administrative staff) of the practitioner; entrusting him with the processing of data does not therefore appear to be a violation of Art. 321 CP. Ideally, the supplier's servers should be located in Switzerland or, at the very least, in Europe (a point of view that is disputed here as to the admissibility of having a supplier outside of Switzerland, but in Europe), and that they are subject to certain certifications as a guarantee of security, such as the ISO27001 standard. Of course, nothing prevents practitioners from having an **internal server duly protected** by a firewall or a VPN when the practice of the profession, especially for lawyers and teleworkers, involves remote work.

- Secondly, **access control** should be put in place, since there is often no justification for all administrative staff to have access to all the potentially sensitive data of the patients treated, or even for each employee to know how much his or her colleagues are paid. The Anglo-Saxon principle of "*need to know basis*" should apply here.

- Finally, one should avoid using unprofessional email addresses, as some in the medical field unfortunately do, such as hotmail, Gmail or bluewin. Moreover, the use of an instant messaging system such as What's App should be avoided in the professional world, except at the express request and agreement (and insistence, I would add) of the patient or client. Email encryption, nowadays easy (see a provider like www.swisssign.com), is to be recommended.

2. **On the information side**

Even though we have seen that the obligation to provide information is in fact confined to the processing of sensitive data (such as medical data) for which express consent is required, it is nevertheless easy and, in my view, good practice to promote a certain transparency here, which can be done with less effort in two ways:

- First, by adopting a **privacy policy** to be displayed on its website or as a flyer in its waiting room, which most often covers the following points: (1) what data is processed; (2) for what purposes; (3) with whom do we share your data? (4) where is it processed, (5) how long do we keep it and (6) what are your rights? This was the choice of Wilhelm Gilliéron Attorneys Corp. which, as a specialist in data protection, could hardly see itself without a policy on the subject, which you will find here.

- Secondly, and more particularly in the medical field where it is usual to have to fill in a **form** before any consultation, the use of this form is a practical and easy way to mention the reason for the collection of certain data (in particular health data for which express consent is required), the way in which they are kept, for what duration and with whom they are shared.

3. **Various**

Finally, it cannot be stressed enough that any transfer of data abroad should only be made with the express consent of the data subject, and that it is important to delete the processed data after a period of time to be determined (usually defined by law) once the data subject is no longer a patient or client (e.g. 20 years for dentists).

4. ***Conclusion***

Although the Federal Data Protection Law and the great media buzz that it generates may be frightening, it is nevertheless easy for those practising in the liberal sector to comply with the applicable requirements by taking a number of measures that are, all things considered, minimal: an adequate privacy policy, a form that makes it possible to ensure express consent in the event of processing sensitive data (even if a signature is not in itself absolutely necessary) and, above all, adequate security measures that only require the taking of measures that are, all things considered, fairly simple.

Source : https://www.wg-avocats.ch/en/news/data-protection/data-protection-liberal-professions/