General Data Protection Regulation: What It Means For US Healthcare/Life Science Companies

Written by Catherine Muyl, Marion Cavalier

August 28, 2017

The clock is ticking: on May 25, 2018, in less than a year from now, the General Data Protection Regulation ("the GDPR") will apply in all Member States of the European Union ("EU") and will replace the Directive 95/46/CE ("the Directive").

The purpose of the Directive was to protect the personal data of individuals to an extent that may seem surprising from a US point of view. The new regulation goes even further, since it is presented as "*an essential step to strengthen citizens' fundamental rights in the digital age.*"

The GDPR is, as its title indicates, a "general" regulation which applies to the collecting and processing of personal data by all kinds of entities in all activities, including in the healthcare/life science sectors, whereas the US has a "sectorial approach" of data protection and a specific act (HIPAA) for health information.

The purpose of this post is to provide a summary of some of the GDPR features that are likely to have the most substantial impact on healthcare/life science related businesses.

Why You Can't Ignore the GDPR

Healthcare/life science companies in the EU are already very much attuned to personal data protection as they handle sensitive data such as patients' details and clinical trials subjects' details. Adapting to the GDPR should be relatively easy for them.

Extra Territorial Effect

On the other hand, one of the major impacts of the GDPR is that it extends the application of European legislation to companies outside the EU. Basically, the Directive only applied to organizations established within the EU or which used equipment within the EU, but not to organizations established outside the EU even if they were conducting activities in Europe.

The GDPR has a much broader scope: it will apply to organizations established outside the EU that offer goods or services to individuals in the EU and/or monitor the behavior of data subjects within the EU (Article 3). In other words, even a US company will have to comply with the GDPR if it targets European consumers or monitors any personal data on European citizens.

Some US healthcare/life science companies not affected by the Directive will now have to comply with the GDPR. They may already have some familiarity with EU data protection rules, due to the requirements for data transfers outside the EU (i.e., the EU-US Privacy Shield or other tools, see below) if they received, for example, personal information collected in the course of clinical trials from a CRO established in the EU. However, the requirements will be more stringent once they are directly subject to European rules.

Data Transfer Outside the EU

The GDPR maintains the same requirements for data transfers outside the EU. Such transfers occur, for example, when persons located in the US have access to data stored in the EU. When personal data collected in the EU is transferred to the US a country which, from a European point of view, does not afford an adequate level of protection, important restrictions apply. Such transfer is forbidden except if the data exporter has taken certain precautions such as:

- Signing the relevant Commission standard clauses
- Adopting Binding Corporate Rules
- Certifying into the Privacy Shield scheme

Increased Sanctions

The GDPR considerably increases the sanctions and penalties in the event of non-compliance. Under the Directive, sanctions were left up to the Member States, which led to discrepancies. For example, in the UK, the maximum fine is currently £500,000, whereas in France, it was until recently 150,000€. Under the GDPR, the maximum amount of financial sanctions is harmonized and increased up to 4% of the total worldwide annual turnover or 20 million euros, whichever is the greater (Article 83). Given this change, compliance with the GDPR should be taken all the more seriously.

New General Features of the GDPR

Some of the GDPR general features may be of particular interest for companies in the healthcare/life science sectors.

One Stop Shop

Until now, groups of companies established in Europe had to deal with as many Data Protection Authorities as countries where they were operating. The GDPR set up the so-called one-stop shop mechanism, which is aimed at simplifying the life of businesses. Indeed, a company established in more than one Member State will have to indicate its main establishment to the Supervisory Authority (formerly called Data Protection Authority) where its main establishment is located and will be in touch with such sole Supervisory Authority, called the "Lead Supervisory Authority", for all its data protection issues in Europe (Article 56).

For the data controller (i.e., the entity that makes the decisions), the main establishment should be the place where the decisions on the purposes and means of the processing of personal data are taken. For the data processor (i.e., the entity that processes the data on behalf of someone else), the main establishment should be the place of its central administration in the EU. This is clearly a more business-friendly provision.

On the other hand, European citizens will be allowed to lodge a complaint not only with the Lead Supervisory Authority designated by the data controller but with the Supervisory Authority in any Member State. The idea behind that is to provide individuals with effective means of redress.

In practice for example, a US healthcare/life science company that has its European headquarters in France will have to deal with the French Supervisory Authority for general data protection matters, but individuals could sue it in the courts of their own Member State.

Appointment of Data Protection Officers ("DPOs")

It is now mandatory for companies to appoint a DPO where its core activities consist of processing operations which require regular and systematic monitoring of data subjects on a large scale or processing on a large scale of sensitive data (Section 4).

The GDPR does not define what constitutes a processing on a large scale, but the Article 29 Working Party (the "WP29") issued useful guidelines on DPOs. According to the WP29, it is not possible to give a precise number, though it recommends that the following factors be considered:

- The number of data subjects concerned – either as a specific number or as a proportion of the relevant population
- The volume of data and/or the range of different data items being processed
- The duration, or permanence, of the data processing activity
- The geographical extent of the processing activity

For example, according to the WP29, the processing of patient data in the regular course of business by a hospital is "large scale" but the processing of patient data by an individual physician is not.

Concerning the responsibilities of DPOs, at a minimum they include: informing the company and its employees on their obligations with

respect to data protection law, monitoring the company's compliance, monitoring privacy impact assessments, cooperating with supervisory authorities and handling data subjects' inquiries.

A DPO may be appointed within the company and carry out other tasks as well (as long as there are no conflicts of interest), but the GDPR requires that DPOs must perform their duties and tasks in an independent manner and with a sufficient degree of autonomy. It means that DPOs must not be instructed how to deal with a matter or whether to consult the Supervisory Authority.

Data Breach Notification

The GDPR introduces a new obligation for companies to notify data breaches to the appropriate Supervisory Authority within 72 hours. And the notification must be documented. Companies will also have to notify the data breaches in question to the affected individuals without undue delay "*when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons*" (Article 34).

This "high risk" is not defined in the GDPR. In our opinion, it will have to be assessed on a case by case basis and the sensitivity of the personal data should be taken into account.

Data Protection Impact Assessment (DPIA)

A DPIA is a process designed to describe the processing of personal data, assess the necessity and proportionality of a processing and to help manage the risks to the rights and freedoms of individuals resulting from the processing.

These assessments are mandatory where a type of processing is likely to result in a high risk to the rights and freedoms of individuals. In particular, it must be carried out where personal data processing involves a "the processing on a large scale of [sensitive data] i.e. including health data (Article 35).

This new obligation is worth mentioning because it will most likely become a frequent task for those healthcare/life science companies which process a large amount of health data. It may become a heavy process that they should prepare for.

GDPR Features that Apply Specifically to the Healthcare/Life Science Sectors

Even though the GDPR is a general regulation, some provisions are expressly addressing the specificities of the processing of personal data in the healthcare/life science sectors.

Specific Categories of Personal Data Relating to Health

There was no definition of health data in the Directive. Now, the GDPR defines "data concerning health" as "personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status" (Article 4).

The core rules on the processing of health data remain basically the same as in the Directive:

- Health related data qualifies as sensitive data as well as genetic and biometric data (two new notions that were introduced by the GDPR)
- The processing of sensitive data is in principle prohibited
- Exceptions are listed, lawful grounds allowing the processing of such data (for example explicit consent)

Exemptions for Scientific Research

The GDPR provides exemptions to organizations that process personal data for scientific research purposes as long as they implement appropriate safeguards which include "technical and organizational measures to ensure data minimization", like for example pseudoanonymization (Article 89).

In particular, the GDPR establishes three data subject's rights:

- **The right to information** under which data subjects have the right to be provided with information on the identity of the controller, the contact details of the DPO (where applicable), the reasons for processing their personal data and other relevant information

necessary to ensure the fair and transparent processing of personal data.

- **The right to object to the processing** under which data subjects have the right to object, on grounds relating to their particular situation, to the processing of personal data, where the basis for that processing is either public interest or legitimate interests of the controller. In case of such objection, the GDPR provides that the controller shall no longer process the personal data unless it demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.
- **The right to erasure of personal data** (also called "**right to be forgotten**") under which data subjects have the right to obtain from the controller the erasure of their personal data without undue delay in some situations such as: if the personal data are no longer necessary or if the data subject withdraws his or her consent (and the only lawful basis for the processing was such consent).

However, organizations that process personal data for scientific research purposes may in certain circumstances override those rights:

- Regarding the right to information and access (where personal data have not been obtained directly from the data subject) if the provision of information involves a disproportionate effort;
- Regarding the right to object to the processing if it is likely to render impossible or seriously impart the achievement of the objectives of that processing;
- And regarding the right to be forgotten if the processing is necessary for the performance of a task carried out for reasons of public interest.

As regards consent, the GDPR also provides a breathing space for research activities that will certainly be useful. It recognizes that it is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects will be allowed to give their consent to certain areas of research or parts of research projects when in keeping with recognized ethical standards for scientific research.

Unfortunately, it is still uncertain what "scientific research" really means. There is only a broad definition of research in the GDPR that encompasses the activities of public and private entities but is unclear exactly how far the GDPR's research exemption will extend, in particular as regards research activities with a commercial goal. Concerning its application to clinical trials, one of the Recitals of the Regulation states that the processing of personal data for scientific purposes should also comply with other relevant legislation such as that applicable to clinical trials.

Conclusion

To summarize, for healthcare/life science companies that are already compliant with the Directive, it will not be a huge effort to comply with GDPR, but the effort is worth making, if for no other reason than to avoid the increased penalties.

On the other hand, for US companies that were not subject to the Directive before, the process for getting compliant by May 2018 will be more complicated, in particular because the US and the EU do not have the same approach of personal data protection and there will be a privacy "cultural gap" to overcome. However, healthcare/life science companies are used to operating in a regulated environment and the new rules will mean mainly more work for those in charge of regulatory or compliance areas.

We have highlighted above some of the GDPR rules that should be of particular interest for healthcare/life science companies. Of course, it is not an exhaustive summary and we advise companies, in particular those which were not subject to the Directive but will be to the GDPR, to conduct a concrete compliance assessment taking into account their own specificities and needs.

Businesses in the healthcare/life science sectors will also be well-advised to maintain a vigilance on potential domestic Member States' legislation that could affect them. Indeed, the GDPR provides that Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.

RELATED PRACTICES

- Privacy & Data Security
