NORTON ROSE FULBRIGHT

Legal update

The impact of the GDPR on clinical trial research

October 2018
Corporate and commercial
Life sciences and healthcare

In April 2016, the European Parliament adopted the General Data Protection Regulation (GDPR) to modernize its data protection legislation. As of May 25, 2018, the Data Protection Directive was thus repealed and replaced by the GDPR, while all member states' legislation became subject to review, to be aligned with the GDPR, leading to major modifications of the rules that prevailed prior to the GDPR coming into force.

For research trials, enacting the GDPR had a number of implications, both for sponsors, contract research organizations (CROs) and trial sites located in the European Union (EU), and for some foreign CROs and sponsors, which now need to comply with various obligations, some of which are outlined below.

Scope

The GDPR directly applies to: **(i)** processing of personal data by EU controllers and processors in the context of their activities, even if the processing does not take place *per se* in the EU, and **(ii)** processing of personal data of EU subjects by foreign controllers and processors offering services or goods to EU subjects or otherwise monitoring their behavior.

For clinical trials, this means the GDPR will govern the trial activities of all EU sites, as well as all local and foreign sponsors and CROs acting as "controller" or "processor" and processing personal data from EU subjects. These GDPR requirements shall apply in addition to those governing the conduct of clinical trials as adopted by the European Commission (EC) and member states, and to any other privacy rules in effect in these member states.

On that note, the GDPR further confirms that EU and member state legislation may restrict the scope of the obligations and rights pertaining to: **(i)** processing and/or accessing personal data; and **(ii)** subjects' right of rectification, erasure, objection, restriction to processing, data portability and automated decision making, insofar as such restrictions are necessary and respect the essence of subjects' fundamental rights and freedoms and any other requirements set forth in the GDPR. As such compliance with the principles set forth below may be tempered.

Conduct of clinical trials

The qualification as "scientific research purposes" has substantial ramifications for various data processing activities. While the GDPR does not define this term and confirms it should be interpreted broadly, some ancillary documentation emphasizes such term shall not be stretched beyond its common meaning to apply to projects other than those set up in accordance with relevant sector-related methodological and ethical standards and good practices.

Processing. Under the GDPR, processing personal data is lawful only if made for one of the limitative purposes set forth in that regulation. On that note, the GDPR expressly provides that processing specific categories of information – such as genetic data and health data – is prohibited. This prohibition is not, however, ironclad; the GDPR confirms such interdiction shall not apply if such processing is, *inter alia*, necessary for research and complies with the rules detailed in the GDPR in this regard.

Additional rules on processing personal data obtained either directly from the subjects themselves or by other means will also apply. These rules notably outline a minimal list of information to be disclosed to these subjects, including: **(i)** the purpose and legal basis for such processing; **(ii)** the period for which such data will be stored; and **(iii)** whether the provision of such data is a statutory or contractual requirement, or is compulsory or non-mandatory. These clarifications must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

Again, these rules will not systematically apply. For instance, a controller that obtained personal data by means other than from the subjects themselves will not be required to comply with its duty to inform if: **(a)** the provision of such information proves impossible or would involve a disproportionate effort; and **(b)** appropriate measures to protect the data subjects' rights and freedoms and legitimate interests are implemented, including by making the information publicly available. In addition, specific provisions to adapt the application of these rules may be introduced in member state legislation.

Finally, should processing involve the transfer of personal data to non-EU countries or organizations, then such transfer must be made to countries or organizations for which an adequacy decision was adopted by the EC or by relying on another provision of the GDPR, provided that member state law may restrict by law of legislative measures data transfer to non-EU countries.

Consent to Data Processing. Where processing is based on consent, the controller must demonstrate that such consent was validly obtained, namely that such consent: **(i)** was presented in a manner clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language; **(ii)** was given for specific purposes clearly identified; **(iii)** remains revocable at any time; and **(iv)** meets all other requirements listed in the GDPR. For research, the obligation with regard to specific consent will apply, but the GDPR allows that such purpose be described more generally in cases where data processing purposes within a specific project cannot be specified at the outset. The relevant provisions of Regulation (EU) No 536/2014 should also apply in addition to the foregoing consent rule or any other rule enacted by each member state.

Secondary Uses. The GDPR expressly provides that personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes. To ascertain whether a purpose of further processing is compatible with the initial purpose, a controller, after meeting the requirements for the lawfulness of the original processing, should take into account: **(i)** any link between the initial purposes and the purposes of the intended further processing; **(ii)** the context in which the personal data has been collected, including subjects' reasonable expectations; **(iii)** the nature of the personal data; **(iv)** the consequences of such further processing for the subjects; and **(v)** the existence of appropriate safeguards in both the original and further processing operations.

Any additional information considered relevant shall be provided to the subjects prior to such further processing, including details on that processing. In addition, the GDPR confirms that exemptions from the foregoing rules may be codified in member state law where personal data are processed for research, and interestingly asserts that for research, such further processing should not be considered incompatible with the initial purposes, provided appropriate technical and organizational measures are implemented.

Storage. The GDPR specifies that personal data shall be kept in a form that permits identification of subjects for no longer than the time necessary for the purposes for which such data was processed. However, this storage limitation will not apply insofar as the personal data is processed solely for scientific purposes, subject, however, to implementing the appropriate technical and organizational measures as required by the GDPR. Additional exemptions may also be found in member state law.

Right of Access. Likewise, data subjects have the right to obtain from the controller confirmation if personal data concerning them is being processed and request access to such data and other information, including the categories of persons to whom such personal data will be disclosed and the envisaged duration of storage. Furthermore, subjects have the right to receive personal data concerning them. In both cases, exemptions may be provided for in member state law insofar as such rights are likely to hinder achieving research purposes and such exemptions are necessary to fulfil those purposes.

Right of Rectification and to be Forgotten. The GDPR provides that data subjects have the right to request, and any controller shall have the obligation to erase, personal data concerning them and stop processing such data without undue delay. Withdrawing consent constitutes a ground giving rise to such right to be forgotten. Likewise, the GDPR expressly states that upon request, subjects shall have their personal data rectified without undue delay. However, the GDPR provides exceptions to these rights, such as the one applicable in clinical trials whereby the right to be forgotten could be overruled if it is likely to hinder achieving the objectives of the personal data processing. Additional exceptions to these rights may be codified in member state law.

Right to Object. Data subjects shall have the right to object at any time to the processing of their personal data in various situations unless one of the exceptions in the GDPR applies. For clinical trials, the GDPR provides that subjects have the right to object to the processing of their personal data on grounds relating to their particular situation, unless the processing is necessary for performing a task carried out in the public interest or another limitation set forth in member state legislation applies.

Security Measures and Data Breaches. As per the GDPR, any controller or processor shall implement technical and organizational measures to ensure a level of security appropriate to the risk of data processing, taking into account: **(i)** the state of the art, **(ii)** the costs of implementation; **(iii)** the nature, scope, context and purposes of processing; and **(iv)** the risk of varying likelihood and severity for subjects' rights and freedoms.

These measures could include, *inter alia* and as appropriate, those listed in the GDPR, such as pseudomization and encryption of personal data. In this regard, the GDPR suggests how compliance could be demonstrated, such as adherence to approved codes of conducts or certification mechanisms.

In addition, the GDPR indicates an impact assessment shall be carried out, particularly when sensitive data will be processed. Records of processing activities under controllers' and processors' responsibility shall also be maintained. Moreover, should transfers of personal data to foreign countries or organizations be required, then such transfers shall only take place in strict compliance with GDPR rules. Finally, the GDPR emphasizes that a data protection officer shall be designated when the core activities of the controller or processor consist of large-scale processing of sensitive data, while an EU representative shall be appointed for foreign controllers and processors.

Regardless of whether adequate security measures were implemented, a controller will be required to notify the relevant supervisory authority of any personal data breach, unless such breach is unlikely to risk subjects' rights and freedoms. Compliance with such obligation shall take place without undue delay and, where feasible, not later than 72 hours after the controller became aware of such breach; any notification not made within that 72-hour period shall be accompanied by reasons for delay. As for the processor, it shall be required to notify the controller without undue delay after being made aware of any breach. Disclosure to subjects will also be required if such breaches are likely to result in a high risk to their rights and freedoms. Considering the sensitivity of the data usually collected by researchers, disclosure to the subjects is likely to be mandatory.

Consequences for failing to comply with the GDPR

In addition to available remedies, data subjects have the right to an effective judicial remedy and/or to lodge complaints with the relevant supervisory authority should their rights be infringed as a result of processing their personal data in violation of the GDPR, and in this regard, could mandate some not-for-profit body, association or other organization to lodge a complaint on their behalf. Any subject who has suffered material or non-material damage from a GDPR infringement shall have the right to receive compensation for the damage suffered.

Supervisory authorities can also impose administrative fines, in amounts up to 20,000,000 Euros or 4% of the total worldwide annual turnover of the preceding financial year, or up to 10,000,000 Euros or 2% of the total worldwide annual turnover of the preceding financial year depending on the nature of the infringement. Imposing such fines must, however, be in accordance with the general conditions detailed in the GDPR, including after giving proper considerations to specific elements.

Future developments

While the GDPR has spent several months in draft format and has been in force for some time, most of the guidance and standard contractual clauses to be elaborated by the EC and each member state to help implement the GDPR are not yet available. The same applies to the codes of conducts and other guidelines to be made available by the relevant associations or other bodies representing categories of controllers or processors. For instance in Quebec work is still underway to revise the ministry of health and social services-endorsed April 2016 "Standard Legal Clauses of the Information and Consent Forms for Clinical Trials." However, some specific health data governance frameworks, such as the recommendation from the OECD Council, have been made available and warmly welcomed.

Pending the final version of these new standard clauses and other guidelines, any organization conducting clinical trial activities that require the processing of personal data shall nonetheless take all necessary steps to ensure their compliance with the GDPR.

In this regard and until these additional clarifications are available, a more conservative approach should be followed whereby strict compliance to all GDPR rules should be favoured. Accordingly, any organization shall first determine if it qualifies as a "controller" or "processor" under the GDPR and further to such determination, identify the measures applicable to its role as controller or processor that should be implemented. In this regard, a non-harmonized approach was taken by various local institutions, some of which have added appendices to their informed consent forms, while others attempt to avoid involving European sites in their multi-centric studies.

While compliance with GDPR requirements remains demanding and to a certain level challenging due, *inter alia*, to the lack of guidance currently available, the above-mentioned exceptions and restrictions as well as those to be provided for in member state legislation should to some extent facilitate sponsors, CROs and sites activities and promote research.

Véronique Barry
Olga Farman

For further information, please contact one of the following lawyers:

> Brian R. Daley	Montréal	+1 514.847.4764	brian.daley@nortonrosefulbright.com
> Olga Farman	Québec	+1 418.640.5852	olga.farman@nortonrosefulbright.com
> Randy Sutton	Toronto	+1 416.216.4046	randy.sutton@nortonrosefulbright.com
> Janet Grove	Vancouver	+1 604.641.4824	janet.grove@nortonrosefulbright.com