SCTO PLATFORMS

The European General Data Protection Regulation (GDPR): Interactions with clinical research

SCTO Regulatory Affairs Platform
April 2019

The latest in data protection in EU

On 25 May 2018, the European General Data Protection Regulation (GDPR; Regulation (EU) 2016/679) came into force, giving data protection in and, under certain conditions, outside the EU territory, a new focus. In parallel, it introduced several new standards. GDPR replaces the European Data Protection Directive 95/46/EC and aims to harmonise data privacy laws across Europe. This regulation applies to the processing of personal data from living individuals (GDPR, art. 2), carried out by data controllers/processors, whether residing in the EU or beyond its borders. It pertains specifically to the processing of personal data of subjects who are residing in the EU while providing them with goods or services, or while monitoring their behaviour (GDPR, art. 3).

GDPR also defines special categories of personal data (previously called “sensitive personal data”, including among others: genetic data, biometric data, health-related data, data revealing racial or ethnic origin, etc.) for which appropriate safeguards must be put in place in order to ensure lawful, fair, and transparent data processing (GDPR, art. 9). Such safeguards include for instance obtaining a free, voluntary, and informed consent, the designation of a Data Protection Officer (DPO), and the coding or pseudonymisation of data.

The primary objective of GDPR is to ensure that the privacy of data subjects is warranted and their personal data protected. For this purpose, GDPR empowers all data subjects with certain rights, through which they can be assured that the data controller is not misusing their personal data. Eight fundamental rights apply to data subjects under GDPR, namely:

1. Right to information (GDPR, arts. 13–14): The data subject is entitled to ask the data controller for information about what personal data (about them) is being processed and the rationale for such processing.
2. Right to access (GDPR, art. 15): The data subject is entitled to get access to their personal data being processed.
3. Right to rectification (GDPR, art. 16): The data subject is entitled to ask for modifications to their personal data, should they believe that this personal data is not up-to-date or is inaccurate.
4. Right to erasure (“right to be forgotten”) (GDPR, art. 17): The data subject is entitled to ask at any time for the deletion of their data, subject to certain rules and exceptions.
5. Right to restriction of processing (GDPR, art. 18): The data subject is entitled to limit the processing of their personal data, also subject to certain rules and exceptions.

6. Right for data portability (GDPR, art. 20): The data subject is entitled to ask for the transfer of their personal data (to themselves or to another controller), in a machine-readable electronic format.
7. Right to object (GDPR, art. 21): The data subject is entitled to object to the processing of their personal data.
8. Right to object to automated processing (GDPR, art. 22): The data subject is entitled to object to a decision based on automated processing.

In addition to the abovementioned new rights held by data subjects, the following changes are introduced with GDPR:

the extraterritorial applicability of the regulation (GDPR, art. 3): GDPR jurisdiction is extended as it applies to all data controllers (including companies or institutions) processing personal data of EU subjects, regardless of the data controller's location;

- the concept of privacy by design (GDPR, art. 25): this concept calls for the inclusion of privacy at the initial design stages and throughout the complete development process of systems that involve processing of personal data;
- the designation of a Data Protection Officer (GDPR, arts. 37–39) is required where processing operations entail regular and systematic monitoring of data subjects on a large scale, or of special categories of data pursuant to art. 9 (thus, including data concerning health)
- significant fines and penalties in case of infringement of GDPR (GDPR, arts. 83–84).

As GDPR is of a general nature, no specific field of application is addressed. This raises potential issues, in particular for clinical research.

Data protection in Switzerland, under revision

In Switzerland, the various aspects of data protection are regulated through the Federal Act on Data Protection (FADP) and respective cantonal laws. Clinical research data protection specificities are covered by the Human Research Act (HRA) and its ordinances (ClinO; HRO). As of end-April 2019, the Swiss Parliament is currently revising the FADP to take account of current technological and societal evolutions and to address the alignment with GDPR. Ideally the revised FADP should bring Switzerland closer to GDPR standards, allowing for a prolonged recognition of Switzerland as a country with an adequate level of data protection (Decision 2000/518/EC; GDPR, art. 45). The revised FADP is expected to enter into force in 2020. In the meantime, the Federal Data Protection and Information Commissioner provides a regularly updated document detailing consequences of GDPR for Switzerland in general.

Data protection in clinical research, generall

As regards clinical research, data protection is intended to ensure that participants' data is handled appropriately, i.e. that the confidentiality of their records is protected (ICH GCP 2.11). Participants' consent – their agreement to participate in a study and for their data to be used in that study and/or subsequent studies – is obtained via consent forms, prior to study enrolment. Specific processes must be established to ensure consent is given freely and can be withdrawn at any stage. The number of staff with access to study data should be limited, to ensure purposeful and appropriate data handling. In addition, study participants hold certain rights regarding the use of their data, such as: viewing their data (HRA, art. 8), having it corrected if inaccuracies are identified, and having it anonymised should they withdraw their consent (ClinO, art. 9; HRO, art. 10). To protect the participants, study data is generally coded at the time of collection.

The European clinical research community has already experienced many concrete changes and identified potential hurdles (see the article by Demotes-Mainard, Cornu, and Guérin highlighted in *Views and Opinions*).

Among them, the newly introduced **“right to be forgotten”** (GDPR, art. 17) raises some challenges to clinical research. Under GDPR, this right means that at any time data subjects have the right to withdraw their previously granted consent to participate in a study, they can also withdraw their agreement to the processing of already acquired data. Moreover, they can request for their data to be deleted (“forgotten”) and used no further. The application of this right in clinical research is problematic for two reasons.

Firstly, it contradicts the GCP requirements necessitating that changes to source data remain traceable, the original entry remains unobscured, and explained, if necessary (e.g. via an audit trail) (ICH GCP 4.9.0). Secondly, the purpose of clinical research itself comes under scrutiny: if data can no longer remain in the database (even in anonymised form) and is prohibited for further use, both the overall quality of research itself could be impaired and study results biased. Moreover, it might affect the safety of the participants asking to be "forgotten", as well as the safety of the study population as a whole (as it might affect safety analyses). Consequently, consideration should be given to clinical trial data, firstly, as being classified as “special” data category under the GDPR (art. 9) and, secondly, relating to the scientific consistency of the trial to elicit derogation (legal exemption) to the subject’s otherwise prevailing right to erasure (in application of GDPR, arts. 17.3.d and 89.1). The current law is, however, not explicit on the application of this consideration.

The implications of GDPR for clinical research in Switzerland

Although GDPR is not directly applicable to Switzerland, its new requirements add complexity. One of the most substantial changes – seemingly simple, at first consideration – carries a substantial impact: the **territorial scope expansion of GDPR beyond EU borders** (GDPR, art. 3). The focus of GDPR is data protection in general, aiming thus to address the (mis)use of data. Territorial expansion is meant to ensure that data controllers respect EU data protection laws for EU residents, irrespective of where the data controllers are based or where the data is processed (for example, on a server located outside of the EU). Nevertheless, this step towards better control of data use and storage may potentially impact clinical research data processes.

A potential illustration relates to (multicentre) clinical trials or study projects for which Switzerland and EU countries are involved: according to the territorial scope expansion, GDPR should be enforced for any EU residents participating in an EU- or Swiss- sponsored trial, even if the location of the trial is in a Swiss centre. Accordingly, in case of non-compliance with GDPR requirements, a trial conducted at sites in the EU (and/or enrolling EU residents as participants) could face the risk of being fined.

Another significant change relates to the formal introduction of a DPO. Despite the clear definitions of the responsibilities of such a DPO, interpretation regarding the details and practical application of their obligations are rather open (GDPR, arts. 37–39). GDPR requires a DPO to be in place where large-scale monitoring is performed, to ensure GDPR is warranted for all participating EU residents. But it is not explicitly defined whether every study centre requires its own DPO and if it is acceptable from an EU point of view for a DPO to reside outside the EU (e.g. at a Swiss sponsor site).

Summary and perspectives

Uncertainties remain in what extent is GDPR really applicable in the context of clinical research in Switzerland. Which potential issues can we expect and which will be the thorniest? How serious is the threat of financial fines to those sponsors who cannot demonstrate clear adherence to GDPR? We still need to

cumulate experience to answer such pending questions.

In theory, Swiss standards are equivalent to EU standards; so the clarification of obligations could be managed through establishing adequate contracts between EU sponsors and their Swiss study sites. But with little room for interpretation, Swiss trial centres might already feel uncomfortable acting with such uncertainties. Luckily, with much progress underway, the coming months will bring greater clarity on these questions.

At the SCTO Regulatory Affairs Platform, we have set up a project team, dedicated to follow closely this topic. Project team: Christina Huf (CTU Bern, Lead), Sonia Carboni (CTU Geneva), Laura di Petto and Cristiana Sessa (EOC Ticino).