Europe Moves to the Next Level in Protecting Personal Data

The GDPR & Research

By Jenny McVey, Life Sciences Manager, Mark Scallon, Life Sciences Partner, FRA

ABSTRACT: As cross-border business and technology advances, the European Union’s need to address data privacy protection continually rises. The General Data Protection Regulation will soon be enforceable and undoubtedly will have impact on how pharmaceutical and medical device companies conduct clinical trials and research studies. This article reviews key updates for companies to consider for their clinical trials and research functions as the May 25, 2018 enforcement date approaches.

After four years of discussion, the European Parliament adopted the European Union (“EU”) General Data Protection Regulation (“GDPR”) in April 2016. With an enforcement date starting May 25, 2018, the GDPR will replace the current Directive implemented in 1995 and will be applicable to Member States. As an EU-wide regulation, the GDPR introduces a single set of rules to allow for consistent data protection standards and enforcement.

While the GDPR preserves the core principles of the Directive, it also introduces clearer and broader definitions, increased data subject rights, and significant penalties for non-compliance (i.e., up to 4% of annual worldwide turnover or €20 million, whichever is higher). Considering that life science companies handle a large amount of personal information such as customer data, patient details, and marketing intelligence, the GDPR introduces significant new compliance obligations.

Clinical trials and scientific research studies are a hotbed of personal data. Although practices to protect participant data are already rigorous, life science companies will need to adapt their stringent procedures to ensure compliance to the new regulation. This article will summarize some of the key areas of the GDPR that will impact studies and provide some insights for life science companies to consider.

Background – Protecting the Privacy of EU Citizens

The European Commission (“EC”) issued the Data Protection Directive 95/46/EC in 1995 to prohibit transfer of EU citizen personal data to non-EU countries that did not have an ‘adequate’ level of privacy protection. More specifically, it required that “personal data shall not be transferred to a country or territory outside of the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedom of data subjects in relation to the processing of personal data”. To bridge the differences in approach to data privacy, the US-EU Safe Harbor Framework (“Safe Harbor”) was developed in 2000 to provide a mechanism to enable free transfer of data between EU and the US. Since then, technological advances and increasing international data flows pushed the EC to recognize the growing need for more consistent and stringent privacy safeguards for EU citizens.

1. FRA Life Sciences offers a broad set of services to help companies identify global compliance risks and develop practical, yet effective, solutions. http://www.forensicrisk.com
2. Data Protection Directive 95/46/EC
Shortly after the EC began to draft the GDPR in 2012, news of Edward Snowden revealing the NSA’s data collection practices, together with an investigation into Facebook’s EU privacy practices (alleging that Facebook did not adequately protect data across borders), compelled the European Court of Justice to review the ‘adequacy’ criteria in the US. As a result, the Safe Harbor was invalidated in October 2015. After those events, the EU-US and Swiss-US Privacy Shield (“Privacy Shield”) was then developed and implemented in July 2016 with the intent of providing more accountability and oversight over data protection privacy than was provided under the Safe Harbor.

During this time, the GDPR was adopted by the EU in April 2016 after a lengthy reform, and will be enforceable May 25, 2018. The aim of this new regulation is to harmonize the obligations of Member States to reduce complexity, provide clearer guidance, and to reinforce data protection measures. Like the Privacy Shield, the GDPR provides to those running clinical trials and research studies specific context around processing personal information while balancing individual rights to privacy and the pursuit of public interest.

**What does this mean for life science companies?**

Since the Directive and GDPR defines a ‘data controller’ as an individual or entity that determines the purposes and means of the process of personal data, many have interpreted life science companies or trial/study sponsors as the ‘data controller’. Although this concept seems intuitive, some would argue clinical research organizations (“CROs”) would instead fall under the definition of the data controller due to their direct role in studies. However, because life science companies determine the nature and purpose of the data collected, one can infer that they fall under the definition of a data controller. Along with hefty fines and penalties, the GDPR additionally expanded certain areas (set out below) that will directly affect life science companies’ process and transfer research data:

**Definition of ‘personal data’ expanded.** Pseudonymised patient data for clinical trials is a common practice and can be done by having identifiers removed and replaced with a unique identification code (e.g., key-code). This privacy-enhancing technique is encouraged by the GDPR, which allows a third-party (e.g., data analyst) to view the data without being able to link it back to a specific participant of a trial. However, by design, pseudonymised data could be traced back to the individual if, for example, follow-up medical attention or verification of data is needed. Because a key-code could potentially be hacked therefore linking the data back to an individual, the GDPR confirms that pseudonymised data must be treated as personal data. Simply put, key-coding alone is not a sufficient technique to exempt data from the scope of the GDPR.

However, many would argue that this creates some confusion for data transferred to the US, as the Privacy Shield states ‘a transfer from the EU to the [US] of [key-coded] data would not constitute a transfer of personal data that would be subject to the Privacy Shied Principles’. Considering the GDPR is a regulation, while the Privacy Shield is a ‘program’ which companies voluntarily join in good faith for the good of business, it can be fair to say that GDPR trumps the Privacy Shield.

**Not all research data is the same.** The GDPR recognizes that some personal data may be more sensitive than others, and therefore carved out certain categories of personal data for clinical or scientific research:

- **Personal data concerning health:** this includes personal data that is ‘related to the physical or mental health of an individual, including the provision of health care services, which reveal information about [data subject’s] health status.’

- **Genetic data:** an individual’s data related to the inherited characteristics, which provides information about the physiology or health of the data subject, such as DNA, RNA, protein markers, etc.

- **Biometric data:** personal data resulting from physical, physiological or behavioral characteristics that confirms the data subject’s identity (e.g., facial images, etc.).

Because studies often require these types of data, the GDPR requires more protection, such as mandatory pseudonymisation, anonymization, encryption, etc., if not already done so.

---

4 Court Justice of the European Union ‘The Court Justice declares that the Commission’s US Safe Harbour Decision is invalid’ Press Release No. 117/15.
6 EU-US Privacy Shield Supplemental Principles, Section III (14)
7 GDPR, Article 4(7)
8 EU-US Privacy Shield Supplemental Principles, Section III (14.g.)
9 GDPR, Article 4(12)
Affirmative consent and the right to be forgotten. The days of presuming that valid consent has been given using pre-ticked boxes, failure to opt out, or inactivity of a participant will be gone. The GDPR requires the data subject to be able to freely provide explicit, specific, and informed consent for processing of their personal data. This means that the purpose, processing activities, how long data will be stored, rationale for data use, potential use of data, etc. should be explained in clear, unambiguous terms – simply put, no legalese or complex scientific terminology. The GDPR also recognizes that it is often not possible to fully identify the purpose of data processing, where the data may be utilized for secondary purposes (e.g., marketing, clinical follow ups, related studies, unanticipated studies, etc.). Therefore, broader consent may be permissible, where study participants should be ‘allowed to give their consent to certain areas of scientific research’. This provision is like that provided within the Privacy Shield, where data in the US may be used for future research, if the study participant is provided clear notice and option to withdraw.

Additionally, the GDPR provides an individual with the right to request the deletion of any personal data, with the expectation that the information will be wiped out ‘without undue delay’. This means that the company will be responsible for finding and deleting any data associated with an individual within their organization, as well as any other area where the data was shared, such as hospitals, CROs, data analysts, health care professionals, etc.

More about transferring personal data. The matter of transferring personal data out of the EU is not new and is further addressed in the GDPR. The new regulation adds that personal data may be transferred in limited situations where the company implemented appropriate safeguards (e.g., binding corporate rules, contractual clauses adopted by the EC, explicit consent, etc.). Additionally, transfers of data may occur outside of the EU when necessary for legitimate purposes, such as public interest, if privacy and rights of the data subject are not violated. However, to make use of this transfer mechanism, the data transfer must: 1) not be repetitive, 2) be for a limited amount of data subjects, 3) have been assessed by the data controller and include documentation of suitable safeguards, and 4) ensure that the data subject and data protection authority (“DPA”) of the relevant member state has been notified.

Enhanced accountability and compliance. Under the GDPR, companies will need to demonstrate measures of accountability and compliance. For example, companies will be required to maintain documentation on the purpose and needs of the data collected, the type and proportionality of data processed, risks, and a data protection impact assessment for ‘high risk’ processing (i.e., large-scale processing of the certain categories mentioned above). Additionally, companies will be required to integrate compliance measures into their data processing activities to show that personal data is protected by design or default (e.g., automatic pseudonymisation).

Some Key Considerations

Life science companies that transfer study data outside of the EU will undoubtedly be impacted by the obligations set forth in the GDPR. However, there is still time to implement provisions to reduce risk.

For example, companies should take steps to better understand their ‘data universe’. This not only means study data, but includes knowing who collects the data, what categories of personal data are collected, where and how the data is stored, how long the data must be kept, used and for what reason, etc. Gaining a better insight into the ‘data universe’ will allow life science companies to better determine the appropriate safeguards.

Another area for companies to evaluate is their governance framework and documentation. Privacy should become a core business program for life science companies. Therefore, a more thorough examination of current privacy practices should take place including:

- Whether the company’s policies and procedures outline the minimum required standards?
- Are the compliance, data privacy or clinical programs assessing, monitoring, and reviewing data collection processes?
- Does the company have appropriate safeguards in place to demonstrate that it has valid consent?
- Does the company have the appropriate safeguards in place to transfer data out of the EU?

10 GDPR, Recital 25(aa)
11 GDPR, Article 17(1)
12 GDPR, Article 44(1)(h) and (6)
Because the GDPR requires information provided to data subjects to be clear, concise, and in plain language, the Compliance or Data Privacy Office should consider developing governance documentation that is easily accessible, easy to read, and understand. This includes procedures on handling personal data, processes to address instances of misconduct, company enforcement standards, and responsible parties.

Since the ability to transfer data is becoming more onerous, life science companies should evaluate their current processes and procedures. Depending on the nature of personal data that is being processed, some of the following questions should be asked about data transfer strategies:

- Does the company know where the data is originating from?
- Is there a need to enhance consent processes for transfer of data?
- Are the safeguards in place sufficient?
- Should the company enhance any corporate rules?
- Are there appropriate contractual clauses in place to meet the GDPR requirements?

It’s safe to say to err on the side of caution, and involve data privacy and transfer experts to better understand cross-jurisdictional laws and regulations.

Additionally, companies should determine the need to designate a data protection officer. Depending on the scale of processing personal data, a data protection officer (“DPO”), who has expert knowledge of data protection laws, regulations, and practices, should be assigned if there is large-scale data processing which 1) processes certain categories of data (personal health, genetic, or biometric data), or 2) requires data subjects to be regularly monitored. How do you know if you have “large-scale” data processing?

Per Recital 91 of the GDPR, large-scale processing activities are those “which aim to process a considerable amount of personal data at regional, nation or supranational level and which could affect many data subjects” and does not apply “if the processing concerns personal data from patient to clients by an individual physician, other health care professional or lawyer.”

Finally, as mentioned previously, CROs may be considered as ‘co-data controllers’, who then would have the same obligations of the company. Companies need to consider re-evaluating their relationship with their CRO’s to ensure each party has a clear understanding of the responsibilities as a controller (e.g., shared responsibility, split responsibility, etc.). This examination could require a more detailed agreement between the company and CRO, specifying the accountability and responsibility of each party.

**Conclusion**

Although we still have a year to comply, there is a lot to prepare for GDPR. The requirements demand a detailed and through compliance approach, particularly given the hefty fines that can be levied for violations. The GDPR introduced a tiered approach to penalties, with a fine of up to 4% of annual worldwide turnover or €20 million, whichever is greater. Thus, the consequences of not complying with European data requirements can no longer be considered trivial.

Furthermore, these penalties could be for a breach of requirements related to transfers of data or non-compliance with the basic principles for collecting data (e.g., consent). The good news is that there is still time for life science companies to evaluate their current clinical trials and research programs. Through the implementation of self-regulating measures, companies can further protect the privacy of the participants, while maximizing the value of the data collected.