ROPES & GRAY

FOCUS ON GLOBAL HEALTH CARE COMPLIANCE

February 14, 2017

The GDPR – Possible Impact on the Life Sciences and Healthcare Sectors

Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016, (the "**GDPR**") came into force in May 2016 and introduced a number of changes to European data protection law. Such changes will impact many entities conducting business within the European Union (the "**EU**"); however, the implications for organizations operating in the life sciences and healthcare sectors are likely to be particularly far-reaching. Life sciences and healthcare-related businesses often collect and/or use large amounts of sensitive health-related data in respect of living individuals, such as patients and clinical trial subjects, so the new data protection requirements will be particularly relevant for them.

We set out below a summary of some of the more significant changes that are likely to impact stakeholders within these sectors.

Extra Territorial Effect

Previously, European data protection legislation only applied to organizations that collected and/or used personal data if such organizations were established within the EU, or if they were established outside the EU, but used equipment within the EU to process personal data (unless this was only for transit purposes).

The GDPR will continue to apply to organizations established within the EU which process personal data; however, organizations established outside the EU will now also be subject to the GDPR if such organizations process the personal data of EU-based individuals and either (i) offer goods or services to individuals within the EU; and/or (ii) monitor the behavior of data subjects within the EU. Any non-EU-based entities to which the GDPR applies will be obliged to appoint a representative within the EU to ensure that they comply with the requirements of the GDPR when processing the personal data of European citizens in the ways set out above.

This means that more non-EU-based organizations operating in the life sciences and healthcare sectors (for example, contract research organizations involved in clinical trials, providers of healthcare services and health insurance companies) are likely to be subject to the GDPR, going forward, than were subject to previous European data protection legislation.

Special Categories of Personal Data

The GDPR prohibits the processing of certain special categories of personal data (or "sensitive personal data"), subject to certain exceptions. The special categories of personal data include, among other things, genetic data and data concerning health.

"Genetic data" is defined by the GDPR for the first time. "Genetic data" includes personal data relating to the inherited or acquired genetic characteristics of a natural person that give unique information about the physiology or health of that natural person and that result, in particular, from an analysis of a biological sample from the natural person in question.

Although data concerning health was protected as a special category of data under the previous EU data protection legislation, the GDPR also defines "data concerning health" for the first time. "Data concerning health" includes personal data related to the physical or mental health of a natural person, including the provision of healthcare services, which reveal information about his or her health status.

Organizations operating in the life sciences and healthcare sectors that collect and/or use any data concerning health, genetic data, or other types of sensitive personal data will need to ensure that they fall within one of the exceptional circumstances set out in the GDPR when the prohibition on the processing of sensitive personal data is deemed not to apply. Among others, these include circumstances where:

i. the individual to whom the sensitive personal data relates has given his/her explicit consent to the processing for one or more specified and lawful purposes (unless such consent is prohibited by applicable EU or Member State law). Obtaining consent from individuals under the GDPR is discussed further below;

ii. the processing is necessary to protect the "vital interests" of the individual to whom the relevant data relate or another individual where the data subject is physically or legally incapable of giving consent (generally, this exception can only be relied on in "life or death" type situations);

iii. the processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of EU or Member State law or pursuant to contract with a health professional and subject to certain conditions and safeguards; and

iv. the processing is necessary for public interest reasons in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of healthcare and of medicinal products or medical devices, on the basis of EU or Member State law that provides for suitable and specific measures to safeguard the rights and freedoms of data subjects, in particular professional secrecy.

It should also be noted that Member States may maintain or introduce further conditions, including limitations, regarding the processing of genetic data or data concerning health, so organizations will need to be confirm whether any such additional restrictions exist in the relevant EU Member States where they process any such data.

Consent

Many organizations and businesses operating in the life sciences and healthcare sectors rely on obtaining the explicit consent of individuals to justify the collection and use of their sensitive personal health-related or genetic data (although this is not the only legal basis for processing of such data that can be relied on). The GDPR introduces a number of additional requirements that must be met to ensure that any consents that are obtained can be relied upon.

The GDPR introduces a new definition of "consent". "Consent" is defined to mean any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or clear affirmative action, signifies agreement to the processing of personal data relating to him or her. Valid consent can be obtained in various ways (e.g., by requiring individuals to sign consent forms, or by clicking on an electronic "I consent" button).

If processing is based on consent, organizations must be able to show that individuals have agreed to the processing of their personal data. Furthermore, if consent is given in a written declaration that also relates to matters other than the consent, the consent request must be presented in a way that is clearly distinguishable from the other matters, intelligible, easily accessible and in clear and plain language in order to be valid.

The GDPR also makes clear the fact that individuals have the right to withdraw their consent to the processing of their personal information at any time (although this will not affect the lawfulness of any personal data processing that was carried out before consent was withdrawn). Individuals must also be informed that they have the right to withdraw their consent before consent is given and withdrawing consent must be as easy as giving consent.

The GDPR also provides that consent is unlikely to be deemed to be freely given where the performance of a contract, including the provision of a service, is made conditional on consent to the processing of personal data that is not necessary in order to perform the contract.

Life sciences and healthcare-related businesses that are subject to the GDPR should consider the procedures and wording that they use when obtaining consent from individuals, for example, informed consent forms used in connection with clinical trials or patient treatment. Informed consent forms that complied with the requirements of the previous EU legislation are unlikely to be adequate to comply with the consent requirements of the GDPR, so these should be updated as necessary to make sure that they are robust. Some commentators have observed that the GDPR's consent requirements are likely to make valid consent difficult to obtain in practice, so it will be interesting to see whether data controllers continue to rely on individual consent or seek to rely on alternative justifications for their processing of personal and sensitive personal data.

Anonymisation and Pseudonymisation

Many life sciences and health sector businesses use coded data, particularly in the context of clinical trials. The issue of whether or not such data constitutes personal data and therefore whether or not European data protection legislation applies to it has long been a controversial topic.

The GDPR defines "pseudonymisation" for the first time. Essentially, pseudonymisation is defined to mean the processing of personal data in such a way that the personal data can no longer be attributed to a specific individual without using additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable individual.

Among other things, the GDPR provides that data protection principles should apply to any information concerning an identified or identifiable individual. It also makes clear that personal data that has undergone pseudonymisation that could be attributed to an individual by the use of additional information should be considered to be information on an identifiable individual (in other words, pseudonymised personal data which allows re-identification of individuals will often be considered to be personal data).

The GDPR provides that, in order to decide whether an individual is identifiable, all the means reasonably likely to be used, either by the relevant data controller or a third party to identify the individual directly or indirectly, should be considered. In deciding whether means are reasonably likely to be used to identify an individual, various objective factors should be considered, for example, the costs of and amount of time required for identification, taking into account the technology available at the time the data is processed and technological developments.

Life sciences and health sector businesses will need to consider carefully whether individuals who are the subjects of any coded data that they collect and/or use would be deemed to be identifiable for the purposes of the GDPR. If so, then they will need to comply with the provisions of the GDPR in respect of such pseudonymised personal data. Certain commentators have observed that effective pseudonymisation of personal data that does not allow re-identification of individuals will be difficult to achieve in practice. Pending further guidance from European regulators on this point, it is probably safer to assume as a default position that any coded data constitutes personal data for the purposes of the GDPR and comply with the GDPR's requirements in respect of such data.

Data Protection Design and Default and Privacy Impact Assessments

The GDPR introduces new formal requirements in respect of data protection by design and default principles. When deciding on a system for personal data processing and also when using that system to carry out such processing, data controllers must now implement appropriate technical and organizational measures, such as pseudonymisation, that implement data protection principles (for example, data minimisation) effectively and incorporate appropriate safeguards into the processing of personal data to meet the GDPR's requirements and protect individuals' rights. The state of the art, costs of implementation and the nature, scope, context and purposes of the intended personal data processing must be considered, together with the risks of varying likelihood and severity for individuals' rights and freedoms that are raised by the processing.

Data controllers must also put in place appropriate technical and organizational measures to ensure that, by default, only personal data that is necessary for each specific purpose of the processing is processed and that by default personal data is not made accessible without the individual's intervention to an indefinite number of people.

Life sciences and healthcare organizations will need to introduce appropriate policies and procedures to ensure that appropriate measures and safeguards are incorporated when introducing new personal data processing systems, products or processes and to ensure that data protection by design and default principles are respected.

The GDPR also formally requires data controllers to carry out privacy impact assessments in relation to any personal data processing that is likely to result in high risks to individuals' rights and freedoms, particularly where the processing uses new technologies. Privacy impact assessments must be carried out, in particular, in a number of specified circumstances, including where personal data processing involves large scale processing of certain sensitive personal data, including genetic data and data concerning health. Privacy impact assessments should include various elements and, where appropriate, data controllers are obliged to seek the views of data subjects or their representatives on the intended processing (without prejudice to the protection of commercial or public interests or the security of the processing).

Life sciences and healthcare organizations should carry out privacy impact assessments in any circumstances when they are proposing to process large amounts of sensitive health-related data (e.g., when designing and running clinical trials and introducing new products and/or services for patients). Potentially, they may also have to seek the views of the relevant individuals or their representatives about their intended personal data processing in these circumstances, at least to some extent.

Data Processors

In addition to imposing new requirements on data controllers, the GDPR imposes various data protection obligations directly on data processors for the first time (data processors include any natural or legal person, public authority, agency or other body that processes personal data on behalf of a data controller). For example, the GDPR extends to

data processors the requirement to ensure an adequate level of protection for personal data that is transferred outside the European Economic Area. Similarly, data processors must put in place appropriate technical and organizational security measures to protect personal data to create and maintain certain records of their personal data processing activities (among other things).

Life sciences and healthcare organizations who are acting as data processors on behalf of data controllers (e.g. contract research organizations acting on behalf of clinical trial sponsors) will need to ensure that they comply with all relevant requirements of the GDPR, going forward.

Group Actions

The GDPR gives individuals the right for the first time to mandate not-for-profit bodies, organizations or associations, which have been properly constituted under the law of an EU Member State, that have statutory objectives in the public interest and which are active in protecting individuals' rights and freedoms regarding protection of their personal data, to take various actions on their behalf. Such bodies, organizations and associations may lodge complaints on the relevant individuals' behalf, exercise certain rights to obtain effective judicial remedies against data protection regulators and data controllers and processors and receive compensation on the individuals' behalf in certain circumstances.

The GDPR thus increases the possibility of "group action" style data protection claims within Europe. Such claims, which may increase the frequency and costs of data protection-related proceedings, could be especially relevant for life sciences and healthcare-related organizations that infringe individuals' privacy rights, given the large amounts of sensitive health-related personal data that such organizations typically collect and use.

Penalties

The GDPR considerably increases the sanctions and penalties that can be imposed on organizations that breach its requirements. In particular, the maximum monetary penalties that can be imposed by European data protection regulators for serious breaches have been substantially increased to up to: (i) €20,000,000; or (ii) 4% of an undertaking's global annual turnover, whichever is the greater.

Clearly, for life sciences and healthcare sector organizations that handle significant amounts of sensitive personal health related data, the imposition of such increased monetary penalties in the event of a serious breach could be highly significant, so ensuring that a robust data protection compliance program is in place will be critical.

Summary of Significant Issues

A checklist of significant issues that life sciences and healthcare sector organizations need to consider is set out below:

- Does the GDPR apply to your organization, even if it is based outside the EU?
- Has your organization established a robust data protection compliance program to ensure compliance with the GDPR?
- Has your organization established a valid legal basis for processing personal data, particularly data concerning health, genetic data and any other relevant special categories of personal data?

- Has your organization updated its procedures, forms and wording for obtaining individual consents to ensure compliance with the GDPR?
- Does your organization use pseudonymised or "coded" data from which living individuals can be re-identified? If so, does your organization comply with the GDPR's requirements in respect of it?
- Has your organization implemented appropriate policies and procedures to ensure that data protection by design and default principles are respected?
- Has your organization implemented appropriate policies and procedures to ensure that data protection impact assessments are carried out where required?
- If your organization acts as a data processor in any circumstances, is it able to comply with its new obligations under the GDPR?

Conclusion

Although officially in force, the GDPR will not be enforced by European regulators until 28th May 2018. The matters discussed above highlight some of the issues that are likely to impact life sciences and healthcare-related organizations; however, there are also other, more general, issues raised by the GDPR that such organizations will need to consider.

Life sciences and healthcare-related businesses should take steps now to ensure that they are able to comply with the new requirements of the GDPR. This should help such organizations to build and maintain the trust and confidence of their customers, business partners, patients and other individuals whose personal data they collect and process and avoid breaches of relevant data protection rules. Organizations that are prepared for the GDPR are also more likely to avoid enforcement action by European regulators, legal action from data subjects, significant monetary penalties and the attendant reputational damage and negative publicity that can result.