Client Update

Epstein Rosenblum Maoz- (ERM)

GDPR and Digital Health

Introduction

Most of us are by now aware of the changes to data protection regulation which came into force on 25 May of this year by virtue of the General Data Protection Regulation (GDPR).

The GDPR introduced several key changes to the previous data protection regulation. Although most of the new regulations apply to digital health companies in the same way as they apply to other types of businesses, there are certain provisions which are more challenging for digital health companies. These are as follows:

1. Consent - Under the GDPR, the processing of health data (defined 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*), which is considered a "special category" of data, is prohibited unless one of several conditions is met. The most common condition is receipt of explicit consent. Digital health companies must therefore ensure that the consent is explicit, informed and freely given and individuals have the right to withdraw consent at any time. The consent must be "specific" and must be "clearly distinguishable" from any other matters in a written document. In addition, request for consent must be "in an intelligible and easily accessible form, using clear and plain language."

2. Data protection officer (DPO) - Both a data controller and processor must appoint a DPO where:
    - the processing is carried out by a public authority or body;
    - the core activities consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
    - the core activities consist of processing special categories of personal data (for example, health data or criminal convictions data) on a large scale. The definition of what constitutes a "large scale" is not clearly defined. Whether or not the processing is being carried out on a large scale must therefore be determined on a case-by-case basis, while taking into account the context of the processing activity.

3. Data protection impact assessments (DPIAs) - The GDPR requires data controllers to carry out a DPIA in advance of any processing which uses new technologies and is likely to result in a high risk for individuals. The GDPR identifies three specific examples where a DPIA would be required. These include:
    - Where the evaluation of personal data regarding a natural person is based on automatic processing, including profiling.
    - Where special categories of personal data (such as, health data) are being processed on a large scale.
    - When systematically monitoring a publicly accessible area on a large scale.

    The guidance provides a set of evaluation criteria to consider when deciding whether to carry out a DPIA, and further states that a DPIA would be required in most cases where two or more criteria are met (for example, processing special categories of data on a large scale).

4. Privacy by design - One of the key changes to be brought in under the GDPR is that of "privacy by design" along with "privacy by default". The GDPR requires data controllers to integrate data protection into their systems and product designs to ensure the inclusion of appropriate technical and organisational GDPR compliance measures into personal data processing means. In addition, data controllers must also implement "privacy by default" measures to ensure that, by default, they minimise the processing of personal data (meaning, they only process the personal data necessary for each specific business purpose). This means that digital health companies are now obliged to take into account data privacy during design and development stages of all projects along with the lifecycle of the relevant data process.

5. Data protection representatives and registrations - A controller or processor that is not established in the EU is subject to the GDPR if it processes personal data of data subjects who are in the EU and the processing activities are related to (a) the offering of goods or services to such data subjects; or (b) the monitoring of their behaviour as far as their behaviour takes place within the EU. Where a controller or processor not established in the EU is subject to the GDPR, it must appoint a data protection representative in the EU. Such data protection representative need only be appointed in one of the member states where the data subjects are based, irrespective of the number of member states in which it offers goods or services and/or monitors individuals. Such representative serves as the contact point for data subjects and the national supervisory authorities.

Some additional changes introduced by the GDPR, which are relevant to all data controllers and processors and are worthy of note are:

- Territorial reach - As noted above, the GDPR has a broad territorial reach as it applies to organisations established in the EU and to organisations established outside the EU who carry out processing activities relating to the offering of goods or services to individuals in the EU or the monitoring of individuals in the EU.

- Rights of data subject - Data subjects have been granted increased rights under the GDPR, including: (a) the right to be forgotten, which gives individuals a right to have their personal data erased in certain circumstances; and (b) the right to data portability, which allows, inter alia, data subjects to request a transfer of their personal data to another provider.

- International transfer of data - The GDPR retains the international data transfer solutions that existed under the Data Protection Directive, but it gives explicit recognition to the concept of approved codes of conduct and approved certification mechanisms as a means to validate international transfers of personal data.

- Notification of data breach - A data controller must notify a Data Protection Authority (DPA) without undue delay and in any event within 72 hours after becoming aware of a personal data breach, and the processor is under an obligation to notify the controller of any data breach without undue delay.

- Enforcement - The GDPR has introduced a more aggressive enforcement approach with fines of up to 4% of a company's annual worldwide turnover or EUR 20 million, whichever is the greater. DPAs also have significant investigative and corrective powers under the GDPR.

In summary, the GDPR has had and will continue to have a significant effect on digital health companies; by introducing the concepts of "privacy by design" and "privacy by default", digital health companies are required to focus on ensuring GDPR compliance during the design and development phases. When you add to this the requirement to appoint a DPO and carry out a DPIA as well as the extra territorial reach of the GDPR and the enhanced enforcement powers of the DPAs, it is clear that there are many new challenges for these companies to overcome in order to achieve and maintain GDPR compliance.

For further information, please contact Simon Marks.

SIMON MARKS

Partner, head of Hi-Tech and Start-Ups

- marks@erm-law.com
- TEL: +972 (0) 3 606 1603
- FAX: +972 (0) 3 606 1603