EU *General Data Protection Regulation* (GDPR) (Regulation 2016/679) – How is this relevant to the Australian Health and Lifesciences Sector?

By Alison Choy Flannigan, Partner and Nameeta Chandra, Associate

Background

On 25 May 2018, the EU *General Data Protection Regulation* (**GDPR**) (Regulation 2016/679), came into effect, replacing the existing 1995 data protection directive.

The GDPR applies to all EU member states and to organisations in countries outside the EU that process data of individuals in the EU. The extended jurisdiction of the GDPR is arguably the most momentous change introduced by the Regulation and is of fundamental importance to the Australian organisations that are now covered by the GDPR.

Australian organisations must consider two important questions:

(i) whether they are covered by the GDPR, and if so,

(ii) whether their current privacy policies and practices reflect their legal obligations under the GDPR.

The Office of Australian Information Commissioner (**OAIC**), has published a useful resource to assist Australian organisations to undertake their obligations under both the GDPR and the *Privacy Act 1988* (Cth) (the **Privacy Act**) (https://www.oaic.gov.au/agencies-and-organisations/business-resources/privacy-business-resource-21-australian-businesses-and-the-eu-general-data-protection-regulation).

What Australian organisations are covered?

The GDPR concerns the processing of personal data of individuals in the EU by a "controller" or "processor" with an establishment in the EU, or if not established in the EU, where:[32]

(a) the processing activities are related to the offering of goods and services to individuals in the EU (irrespective of whether payment is required); or

(b) if they monitor the behaviour of individuals in the EU (Article 3).

[32] Essentially, a "controller" refers to the natural or legal person, public authority, agency, or other body, alone or jointly with others, that determines the purposes and means of processing personal data, and the "processor" means the natural or legal person, public authority, agency, or other body that processes the personal data on behalf of the controller. (Article 4) The example given is that of a bank (the controller) that collects personal data from a customer for purpose of opening a bank account, and then provides it to another organisation to store (the processor).

Importantly, where the Privacy Act applies to the Commonwealth government, private sector organisations with an annual turnover of more than $3 million and all private health service providers, the GDPR has extended application as it applies to Australian organisations of any size where their activities are captured in Article 3.

The OAIC has provided examples of when an organisation may be covered by the GDPR, including where:

- an Australian business has an office in the EU;
- an Australian business' website targets EU customers (such as by allowing them to purchase goods and services in a European language and / or to affect payment in euros);
- an Australian business website mentions customers or users in the EU; and
- an Australian business tracking and profiling individuals in the EU.

Other examples of Australian organisations covered include universities which have campuses in the EU or maintain contact with alumni residing in the EU.

For the Australian health and lifescience sector, the GDPR may apply to:

- the monitoring of behaviour of individuals in the EU, for example, if an Australian company is the sponsor or the lead international site/co-ordinator of a clinical trial in a European country;
- pharmaceutical or medical device companies who have an office in a European country; or
- the offer for sale of therapeutic goods (including medicines, medical devices and complementary medicines) directly or indirectly through the internet targeting people who reside in a European country.

Key concepts and obligations

The GDPR uses the concepts of "**personal data**" and "**processing**" (Article 4), which are defined as follows:

- personal data means any information relating to an identified or identifiable natural person; and
- processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as the collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination (or otherwise making available), alignment or combination, restriction, erasure or destruction of personal data.

Some of these concepts are reflected in the Privacy Act in relation to the collection, storage, use, disclosure, security and disposal of personal and sensitive information.

The requirement of "consent" is present in many of the responsibilities in the GDPR. Article 4 of the GDPR defines consent as "…freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".

The data controller needs to be able to demonstrate that the individual has consented to the processing. Consent is not freely given if the individual has no genuine or free choice or is unable to refuse or withdraw consent at any time (Article 7 and recital 42). Businesses also need to make the withdrawal of consent as easy as giving consent, and before individuals give consent, must inform individuals about this right to withdraw consent (Article 7(3)). When consent is given in the context of a written declaration, which also concerns other matters, it is to be clearly distinguishable from other matters and provided in an intelligible and easily accessible form using clear and plain language (Article 7(2)). Specific requirements apply to children's consent.

The OAIC recommends that Australian organisations covered by the GDPR standardise their consent mechanism, so it reflects their obligations under both the GDPR and the Privacy Act.

The GDPR also introduces the following new and expanded rights for individuals:

- the erasure of data (or the right to be forgotten): Article 17
- the right to data portability – transporting data between controllers without hinderance: Article 20; and
- the right to object to the processing of data: Article 21

There are no equivalents to these rights in the Privacy Act, although Australian Privacy Principles (**APP**) may contain these rights in some form, for example APP 11.2, provides that APP entities must take reasonable steps to destroy or de-identify personal information that is no longer needed for a permitted purpose.

Other important obligations under the GDPR include mandatory data breach notification without undue delay and, where feasible, not later than 72 hours where a data breach is likely to "result in a risk for the rights and freedoms of individuals" (Article 33).

The GDPR requires data controllers to give individuals a range of prescribed information about the processing of their personal data (Articles 13 and 14).

Penalties

The GDPR imposes substantial fines for organisations that fail to comply with the Regulation. In relation to breaches of certain articles a maximum fine of 20 million EUR, or up to 4 percent of the total worldwide annual turnover of the organisation (whichever is higher) may be imposed (Article 83).

Approach

The recommendation for organisations is to avoid an alarmist approach to the Regulation as many organisations have already been required to comply with various privacy laws, whether in the EU under the existing 1995 data protection directive, or in Australia under the Privacy Act (or any of the state-based privacy laws). It is now just a matter of carefully reviewing those policies and practices to identify any "gaps", and to amend as required.