EU General Data Protection Regulation for Superannuation Trustees to consider

What is General Data Protection Regulation?

The European Union (**EU**) General Data Protection Regulation (**GDPR**) comes into effect on 25 May 2018 and will introduce stringent privacy and data protection requirements on businesses. Many Australian businesses, including Australian superannuation funds, could be affected by the new regulatory regime.

The GDPR will apply to any business established in the EU, and to Australian businesses (including public sector entities) of any size that holds, controls or processes personal data of individuals located in the EU where those activities relate to:

- the offering of goods or services to those individuals (irrespective of whether payment is required); or
- the monitoring of their behaviour as far as that behaviour takes place within the EU.

The consequences of non-compliance are severe with fines of up to €20 million per infringement or 4% of global annual turnover (whichever is greater) and the risk of reputational damage, class actions and other regulatory attention.

The GDPR applies to data controllers (eg trustees of superannuation funds and employers), but also to organisations that process data on behalf of the controller (such as administrators and payroll processors).

Superannuation funds may be unknowingly affected where their members are based in the EU or where they have EU employees. Accordingly, superannuation trustees should consider the personal information they collect or process (especially to identify any members who are located in the EU) and determine whether and to what extent they will need to update their privacy and data protection frameworks to ensure they meet the requirements of the GDPR.

Implications for superannuation trustees

The GDPR is one of the most comprehensive pieces of privacy legislation developed by any jurisdiction to date and goes beyond the requirements of Australia's current privacy regulations. It also confers new rights for individuals. It will apply to all personal information collected including membership information such as identity characteristics, contact details, tax file number, salary, insurance, employer and beneficiaries.

pwc

Where GDPR applies, it is important to be aware of some of the key GDPR impacts for superannuation trustees which include:

1 **Privacy notices**: The GDPR introduces increased disclosure requirements, which must be included in notices to individuals before data is collected. Trustees will need to review and update their existing privacy notices so they are concise, easily accessible, in clear and plain language and include (without limitation):

- the categories of personal data collected
- the intended purpose(s) for processing the personal data
- legal basis for processing the personal data
- intended recipients of the personal data
- retention period of data; and
- members' rights to request access to, correct or delete personal data.

2 **Consent and legal basis for processing**: The GDPR will impose strict requirements for obtaining and relying on consent as the legal basis for processing personal data. Consent must be freely given, be specific, informed and unambiguous. Further, an individual must be able to withdraw consent at any time, as easily as he or she could give consent. This requirement may be impractical for many superannuation funds to comply with. Trustees should review existing consents to see whether they are adequate and if not, identify a legal basis for processing the personal data (eg. processing may be necessary for the performance of a contract with the individual, to protect the vital interests of an individual or for the purposes of legitimate interests pursued by the trustee (or a third party)). Personal data collected should be limited to what is necessary for the purposes for which it is processed and so any data collection beyond this should be discontinued.

Trustees should also assess whether they should continue to rely on existing consents or whether there are other lawful bases under the GDPR for processing personal information.

3 **Processing of sensitive personal data**: Certain special categories of data (eg. religion, trade union membership) will be subject to more stringent protections and the processing of these categories of data will only be allowed in specified circumstances, such as if the individual has given explicit consent. Trustees and their service providers (including third and fourth parties) may therefore need a member's explicit consent before processing health data in connection with a member's application for early access to their superannuation due to terminal illness or temporary or permanent incapacity.

4 **Dealing with data breaches**: A data controller must notify the relevant supervisory authority of any data breach within 72 hours of becoming aware of it (or provide reasons for the delay), unless the breach is unlikely to result in a risk to the rights and freedoms of individuals . The controller must also notify the individual of the breach without undue delay, where the breach would likely adversely affect the individuals involved. Data processors also have an obligation to notify any breach to their controller.

5 **New member rights**: Members will have the right to access (through a Subject Access Request (**SAR**)), be forgotten, and restrict the processing of personal data. Members will also have the right to data portability (ie a right to access their data in machine-readable format or to have the data transmitted from one controller to another). Policies and procedures will need to deal with these requests particularly SARs, as organisations have only 30 days to comply with such requests.

6 **Contracts with third parties**: The GDPR changes the legal relationship between controllers (eg. superannuation trustee) and processors (eg. superannuation administrator, gateway provider, financial advice provider, member portal provider) and requires certain provisions to be included in any such contracts. Processors will have direct obligations to comply with the GDPR and be accountable for their own level of security of data and the manner in which they assess, document and conduct their data-processing activities. Controllers will have related obligations to ensure that the data processors provide sufficient guarantees that the processing will be conducted in accordance with the GDPR's requirements. Where there are joint controllers, the contract must specify the allocation of their responsibilities. Contracts with third parties will therefore need to be reviewed and amended which could take some time. New contracts will also need to be prepared with these new GDPR requirements in mind.

7 **Accountability and record keeping**: The GDPR requires controllers and processors to demonstrate compliance with the GDPR. Trustees will need to update their policies and procedures to reflect the specific obligations they have under the GDPR and implement measures to achieve compliance. Trustees must ensure their records are detailed including the registers of the personal information they collect and process, the purposes of the processing, the categories of recipient of the personal data, any transfers of personal data to a third country, anticipated timescales for deleting and any security measures in place.

8 **Data Protection Officer**: The GDPR introduces a requirement to appoint a Data Protection Officer (**DPO**) in certain circumstances including where the core activity of a controller or processor consists of large scale processing of special categories of personal data. Processing data such as details of spouses (which could indicate sexual orientation) may fall into this category, however, this may not be seen as a core activity. The Trustee may voluntarily appoint a DPO where not required to do so but a voluntarily appointed DPO will have the same status under the GDPR as any other DPO.

Are you prepared?

With the 25 May 2018 enforcement date looming, superannuation trustees should undertake an immediate assessment to determine the scope of impact of the GDPR on their operations and if applicable, begin fast-tracking necessary steps to ensure compliance with the new regime. This will require having good insight into the type of data being collected, and how this is processed (internally and externally). Particular importance should be placed on any third party agreements, communications with members, and ensuring effective measures are in place to monitor, detect and report data breaches.

Our final thoughts…

The GDPR aims to ensure greater accountability and transparency in the information-handling practices of all businesses. The regulation has been introduced in an environment of increasing international regulation of privacy (including, for example, the Australian notifiable data breaches regime which came into effect on 22 February 2018).

The Australian notifiable data breaches regime (as well as the GDPR if it applies) will require Superannuation Trustees to put in place effective data breach response and notification processes. Importantly, these new laws require businesses to be proactive and respond quickly and effectively to data breaches and suspected data breaches.

This is a business imperative and legal compliance is only part of a superannuation funds data protection program. These new regulations present superannuation funds with an opportunity to engage with its members on privacy protection and to build / maintain trust in an increasingly digital world. This is an ideal time to review how your Fund manages its information (and manages itself) to take stock of its key information assets, its data protection measures (including response activities), and to ensure it minimises the risk of a breach in the first place.

PwC looks at data protection as a "whole of business" requirement. We advise our clients on compliance risk reviews and legal advice, third party supplier risk assessments, process development and reform, technology solutions and operational design. If you have any questions about the GDPR, and the ways it may affect the whole of your business, let's talk…

For a deeper discussion on how this regulation may affect you organisation, please contact:

Craig Cummins
Partner, National Superannuation Leader
(02) 8266 7937
craig.cummins@pwc.com

Nicole Oborne
Partner, Superannuation
(03) 8603 2914
nicole.oborne@pwc.com

Sylvia Ng
Director, Legal
(02) 8266 0338
sylvia.ng@pwc.com

Adrian Chotar
Partner, Legal
(02) 8266 1320
adrian.chotar@pwc.com

Lynda Reid
Director, Legal
(02) 8266 3339
lynda.reid@pwc.com

Julie Comninos
Senior Associate, Legal
(02) 8266 5861
julie.comninos@pwc.com