General Data Protection Regulation (GDPR)

Australian payroll functions and outsourced providers need to be aware of European privacy rules too

On 25 May 2018, a stringent and uniform privacy and data protection regulatory regime (the General Data Protection Regulation, or "GDPR" for short) will come into force in Europe, which is more prescriptive than the privacy laws in Australia. So, from an Australian payroll perspective – why should we care? It's Europe, not Australia.

1. Do the rules apply to Australian payrolls?

The GDPR applies to any business (or public sector entity) that holds, controls or processes personal data of EU residents regardless of the business's location. This means that any Australian company that holds personal information of EU resident employees will be captured. Businesses with EU subsidiaries or employees seconded to Europe, or businesses that operate global payroll operations will therefore need to consider their payroll practices to address this new regime. In addition, outsourced payroll providers (who may process data on behalf of such businesses) will also likely need to adapt their practices to comply.

2. Given Australia's had privacy laws for almost 20 years, aren't Australian employers well positioned for GDPR?

Well yes, however, there are key differences between the two pieces of legislation including, significantly, with regard to the employer exemption. In Australia, there is an exemption under the Privacy Act 1988 (**Privacy Act**) for a private sector employer handling employee personal information. There is no such exemption under the GDPR. All personally identifiable information of individuals located in the EU will fall within the scope of the regime. Many Australian businesses may therefore be unknowingly required to ensure that their data handling practices comply with the new GDPR requirements (including employers handling their employees' personal information).

How else do the GDPR rules differ?

The GDPR is one of the most comprehensive pieces of privacy legislation developed by any jurisdiction to date and goes beyond many of the requirements of Australia's current privacy regulations. It also introduces new compliance duties and confers new and enhanced rights for individuals.

The GDPR goes beyond Australia's privacy rules in the following areas:

1. **Consent –** Due to the nature of the employer/employee relationship, an individual's consent may not be sufficient approval for processing employee data. There is a presumption that an individual's consent has not been freely given where there is a clear imbalance in choice between the individual and the data controller. Accordingly, an assessment will need to be undertaken by the employer to ensure that there is another lawful basis for processing employee information.

2. **Transparent collection or privacy notices –** The GDPR imposes a stricter requirement of disclosure to employees before collection of data. These new privacy notices must include (without limitation):
   - the categories of personal data collected;
   - 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
   - employee's rights to request access to, correction or deletion of, personal data.

pwc

3. **Employee rights –** Employees will have the rights to access (through a Subject Access Request), correct, erase and restrict the processing of personal data. Employees will also have the rights to data portability.

4. **Increased protection around collection of sensitive personal data –** Certain categories of information (eg. religion, biometric data and trade union membership) are subject to more stringent protections and employers will be prohibited from processing such data unless it falls within an exception.

What are some of the actions that employers can take to address the new GDPR requirements?

Businesses should undertake an initial assessment to determine the scope of impact of GDPR on their payroll processes. It is possible that new policies or processes will need to be put into place to ensure that required consents are gathered before private data is collected and that effective measures are in place to monitor and detect data breaches. Particular importance should also be placed on any third party agreements and data transfers outside the EU.

1. **Basis for processing employee data** – Employers and payroll processors will need to ensure that they are not processing data which is not strictly necessary for the performance of their duties. Collection of any "non-essential" data, if discovered, should be discontinued as breaching the "data minimization" principle.

2. **Security of payroll information** – The payroll function will need to update its processes to ensure they meet the information security requirements of the GDPR – for example, meeting timeframes for the destruction of personal information and for the mandatory data breach notification requirements.

3. **Visibility over employee data flow** – as employee data may be held on various systems, including recruitment systems, HR systems, corporate registers and third party payroll systems, it will be important to understand the data flows. Payroll functions will need this information to help businesses when responding to employee access requests, data breaches and for reporting purposes under the GDPR.

4. **Transfer of data outside EU** – ensuring appropriate GDPR data transfer mechanisms are in place for any cross-border transfers of data businesses, especially where payroll processing occurs in Australia for any EU-based employees.

What are the consequences of non-compliance?

The consequences of non-compliance are severe with fines of up to €20 million or 4% of global annual turnover (whichever is greater) and other risks (for example, audits, compensation rights, class actions, regulators seeking orders to cease activity).

While we don't know how active the authorities will be in Australia (as the GDPR was formally adopted by the EU in 2016 and businesses have been given a 2 year period to prepare, respond and comply) it is highly likely that the Supervisory Authorities will swiftly seek to enforce compliance from large employers both within Europe as well as overseas.

For further information on navigating the GDPR regime in HR and payroll, please contact:

Adrian Chotar
Partner, Legal
+61 (2) 8266 1320
adrian.chotar@pwc.com

Sylvia Ng
Director, Legal
+61 (2) 8266 0338
sylvia.ng@pwc.com

Peter Malan
Partner, Assurance
+61 (3) 8603 0642
peter.malan@pwc.com

Tony O'Malley
Partner, Legal
+61 (2) 8266 3015
tony.omalley@pwc.com

Rohan Geddes
Partner, Payroll Consulting
+61 (2) 8266 7261
rohan.geddes@pwc.com