The 25 May 2018 deadline for the enforcement of the EU General Data Protection Regulation (GDPR) has now passed, and the increase in instructions received over the last 6-8 months in particular has been a clear indication that organisations are taking the change seriously. From enterprises reviewing the scope of their own regulatory compliance obligations, VCs investing and collaborating with start-ups assessing the risks, to the rise in flow-on compliance obligations from EU customers and suppliers to Australian organisations – all have raised the GDPR flag for many Australian organisations who are keen to understand what the Regulation means for their business – both current and future activities.

Broad extra-territorial application and scope of defined ‘personal data’

Due to the extra-territorial application of GDPR, Australian organisations that collect, process or use personal data from individuals in the EU are subject to the regime. This can be online or offline, and placing cookies on an enduser’s device which monitors or tracks that individual’s movements in the EU may be sufficient to bring an Australian organisation within its remit – even in some cases where the monitoring is completed under a contracted services arrangement. The scope of personal data under the GDPR is broad – it includes any data set which can identify or single out an individual, and is much broader than the Australian definition of personal information. By way of a change to the existing EU regime, biometric and genetic data sets are called out as special categories of data, the processing of which is prohibited unless an exemption can be identified – in many cases this will require the explicit, informed and unambiguous consent of the individual before processing. But there cannot be any imbalance when obtaining that consent, which must be unbundled from other notices and terms provided to individuals. There is no threshold for applicable organisations (similar to the AU$3m requirement under Australian privacy laws) which has the potential to profoundly impact SMEs and new market entrants in the technology start-up space in particular, who seek to do business with EU organisations or enterprises that engage with EU providers in their chain of supply. Successfully navigating these challenges is becoming increasingly difficult for many organisations. Further, contrary to popular belief, public sector entities are not immune. While there are some notable exemptions for public authorities in the area of the prevention, investigation or persecution of criminal offences or criminal penalties, including public and national security and for matters outside the scope of EU laws, the regime has broad application to all public bodies, potentially including those who engage in commercial activities and services.

Liability and an individual’s right of redress

The GDPR brings with it the potential for joint and several liability for controllers and processors brought under its remit (as those terms are used in the Regulation), as well as enhanced rights for individuals. So, for Australian organisations processing data on behalf of an EU customer, an individual whose data has been compromised as a result of an unauthorised disclosure or breach can choose to take recourse directly against the Australian
In the event of a security incident leading to a material data breach, for example, it is not unlikely that, under GDPR, fines would be imposed on the organisation coming under its remit with the potential for direct liability of the Australian organisation if it participated or had knowledge of the breach, and/or joint and several liability with EU customers. Data protection rights are enshrined in the Charter of Fundamental Rights of the European Union and these rights have been actively enforced by regulators and the courts around the world under the current regime so it would not be inconceivable that every effort would be taken to ensure compliance where warranted.

**Enforceability and Take-up**

The take-up in Australia had been decisively (and perhaps not surprisingly) slow, with many organisations appearing to take a ‘wait and see’ approach to compliance. However, this approach has changed in recent months and many global organisations in particular in Australia have heeded the warnings on GDPR. This has no doubt been spurred on by global movements on privacy, including recently publicised high profile data breaches as well as profiled changes in regulation around the world. The latter includes recent announcements in California (which propose a similar, and enhanced regime to EU GDPR); a new mandatory data breach notification regime proposed in Singapore (with minimum hourly notification requirements); changes in South Carolina’s telemarketing laws; new data brokerage laws in Vermont, US – to name but a few. Questions on enforcement in Australia and the likelihood of any proactive regulator investigation or enforcement outside of the EU still pervade – but the risks on brand and reputation, coupled with a desire for Australian industry to ‘lead from the front’ on issues of privacy around the world, have ensured that compliance with GDPR is no longer seen as a ‘nice to have’ for many.

**Current Climate**

Whilst we have yet to see any serious fines for data breach being imposed by EU regulators since the Regulation coming into force three months ago, the significant increase in notifications being received across the continent has confirmed that many organisations are not taking chances. We have also seen a replication of effort in the Australian market here of late following the adoption of the Notifiable Data Breach Regime in February this year. Perhaps not the desired result for many regulators – who run the real risk of ‘notification fatigue’ and resource issues being experienced by their offices – and may in fact have the opposite impact if more serious breaches do not receive the attention warranted by their scope. The recent events surrounding Cambridge Analytica/Facebook disclosures, Dixons Carphone compromised data, Reddit’s hacking issues and Page-Up’s breach closer to home have resulted in security and cyber issues being front of mind for the board at enterprise-scale and similar Australian organisations. We are also seeing increased interest in the litigation funder community for potential class actions, for example, for alleged breach of Section 18 of the Australian Consumer Law (misleading and deceptive conduct) based on representations which may be made by an organisation in their privacy policies or other online forms. There are further challenges around continuous disclosure obligations and directors’ duties implications which are agitating a number of our clients in Australia. From a contract perspective, Australian organisations have also already begun to see this being manifested in agreements with EU customers and suppliers where additional due diligence and assurances on security, data, governance and compliance policies and procedures are being required in an effort to discharge compliance requirements. Detailed data processing addendums incorporating wide indemnities for breach are also now increasingly being proposed for review in the market. The broader social and political concerns arising from recent high profile data breaches, coupled with an ever changing global landscape on privacy, has fuelled a desire for organisations to begin their data mapping audits and review their propensity for liability under the GDPR sooner rather than later; many in an effort to increase their general maturity on privacy compliance.

**AUTHORS**

*Sinead Lynch*
Sydney | T: +61 2 9286 8000
sinead.lych@dlapiper.com
DLA Piper is a global law firm operating through various separate and distinct legal entities. Further details of these entities can be found at www.dlapiper.com. This may qualify as