GDPR: 6 MONTHS ON – WHAT'S CHANGED?

Authored by Tim Gole, Nikhil Shah, Edward Davidson and Bryce Craig

On 25 May 2018, the European Union (EU) (and perhaps less so, the rest of the world) welcomed the introduction of the General Data Protection Regulation (GDPR). Described as the most significant overhaul of data protection laws in recent memory, the GDPR has caused large and small entities around the world to stop, reconsider and, in most cases, re-calibrate their data handling and management practices. But what has changed in practice?

This article reflects on our learnings over the past half year: how we have seen Australian organisations manage their compliance obligations, what we are currently seeing in terms of enforcement, some of the intended and unintended consequences we have seen the GDPR have, and what we might expect to see in the coming months and years.

2018

WHAT DOES IT DO?

The GDPR imposes a number of strict requirements on organisations that process, or control the processing of, personal data of EU persons, including:

+ introducing a mandatory data breach notification regime (Articles 33 and 34);
+ imposing tighter conditions and requirements in relation to obtaining consent (Articles 7 and 8); and
+ formalising the requirement to conduct data protection impact assessments (Article 35).

The regulation also empowers EU persons by giving them rights to:

+ access their personal data (Article 15) and to rectify it where incorrect (Article 16);
+ be 'forgotten', i.e. the erasure of their personal data (Article 17); and
+ object to instances of collection or processing for direct marketing purposes (Article 21).

Most notably, as many of our readers will be all too familiar, the territorial scope of the GDPR is incredibly broad. The regulation captures within its net not just the (expected) big global players. It also captures any organisation (whether established in the EU or not) processing (or controlling the processing of) the personal data of persons who are in the EU where the processing relates to offering them goods or services or monitoring the behaviour (as far as such behaviour takes place within the EU).

WHAT MIGHT HAPPEN IF YOU DON'T COMPLY?

You could find yourself in hot water, with breaches of "higher severity" obligations potentially leading to fines of up to the greater of 4% of the organisation's annual global turnover or €20 million (AUD 31.8 million) (Article 83) – although, six months in, it is unclear what the penalties will look like in practice.

For more background information on the GDPR, including as to its extra-territorial reach and the key changes introduced by it, as well as a comparison of its key requirements versus those under the Australian Privacy Act, please see our "GDPR: The Final Countdown" and "GDPR: Ready or Not, Here it Comes" articles.

A VIEW FROM THE FIELD: TIM GOLE AND NIKHIL SHAH

Q: Do you think the GDPR has generally been well received in Australia?

It has certainly been met with a lot of interest from organisations across the spectrum. The GDPR is a sea-change compared to the obligations imposed by the *Privacy Act* 1988, and a lot of our clients have spent the last 6 months coming to terms with the new regime and asking themselves (and us!) difficult questions about whether the GDPR applies to them and, if so, what they may need to do to comply.

Some have questioned the right of the EU to impose a law that attempts to apply so broadly from a jurisdiction perspective. It really does depend on the circumstances and attitude of the particular client.

Q: Which types of Australian organisations have been coming to you for advice?

Given the GDPR's global reach and how broadly its obligations are framed, we have seen every type of organisation from small charities to multi-national banks and telecoms providers grappling with their obligations under the GDPR. For some of those organisations, this has proven to be a good opportunity to reflect and renew their general data privacy practices regardless of whether or not they are actually subject to the GDPR.

Q: What have they been asking you? How have you been able to assist them?

As Australian lawyers, our ability to advise on the substance of the GDPR is unfortunately limited. However, we have been able to assist our clients in determining whether or not the GDPR applies to their activities. More often than not, the answer isn't black and white, such as where they have no establishment in the EU yet have some EU customers. And where our clients do decide that the GDPR is relevant to them, we work closely with law firms in Europe to assist our clients with their ongoing compliance activities.

Q: How have you see Australian organisations manage their obligation to obtain consent?

We've seen a real range of approaches taken by different types of organisations, with the general trend seemingly that the closer the nexus to the EU (whether physically or as a result of a global client base), the more comprehensive the efforts to obtain explicit and informed consent. At the one end of the spectrum, we have seen large internet service providers reach out to all of their users seeking explicit consent to the ongoing processing of personal data. At the other end, we have seen small retailers take a more pragmatic view that ongoing marketing activities are in the legitimate expectations of their clients, such that consent does not need to be sought.

Most Australian-based organisations seem to fall somewhere in the middle of that range, using a combination of legitimate interests and opt-in consents to manage their compliance and risk.

Q: Has any particular industry been more affected than others?

Strictly speaking, the GDPR is industry agnostic; however, its subject matter naturally leads it to being relevant to certain types of industries more than others. The organisations we have seen grappling most intently with the new regime are those whose business model relies on and/or monetises personal data, including those in the banking, health care and social media spaces.

Q: In your opinion is it likely that Australian organisations without a permanent establishment in the EU will be targeted by regulators?

Whilst of course we wouldn't suggest that Australian organisations are entirely safe from the reach of EU regulators (given the broad powers the GDPR gives them), considering their limited bandwidth and budget, coupled with the practical difficulties of enforcing judgments overseas, they might be expected to focus in the first instance on the "low hanging fruit" in the EU itself. However, this assessment might be tested in the near future (see the recent UK ICO enforcement action taken in respect of a Canadian entity, described overleaf), and "high risk" Australian organisations certainly shouldn't pause their compliance programs in reliance on this.

Q: Do you think there's value for those organisations who aren't required to comply with GDPR to follow the practices of those that do?

Only within reason and subject to other prevailing pressures and budgetary constraints. Ultimately expectations around privacy and data security are only going to increase, so being ahead of that curve, whether forced or not, can't be a bad thing. But at the same time, full compliance with the GDPR is a costly and resource-intensive exercise – it is not just a matter of updating a privacy policy. So being judicious in deciding which aspects to comply with and to what extent is key.

Q: Do you expect to see more guidance published by the regulators in the near future, clarifying the interpretation of some of the key concepts in the GDPR?

I hope so! As a lawyer, it is sometimes difficult to advise clients with complete certainty in this space given the incredibly loose way in which some of the key concepts underpinning the GDPR are drafted (take "establishment" for example, which has no definition in the text) – especially given that many of our clients are organisations for whom the GDPR's relevance is not immediately apparent. I am optimistic that when the dust settles, the regulatory bodies and, in time, the courts will provide us with the clarity that we are after.

Like many things privacy-related, often obtaining precise answers can be difficult, and a significant degree of judgment needs to be exercised. Regardless of whether we are talking GDPR or the Australian Privacy Act, reputational issues always need to be front of mind.

THE ENFORCERS AND THEIR ENFORCEMENTS

The introduction of the GDPR has resulted in the creation of a new body, the European Data Protection Board (**EDPB**), which replaces the Article 29 Working Party and is made up of the data protection authorities (**DPAs**) of the EU Member States. However, the EDPB is not an enforcement authority; rather, it acts as a facilitator which seeks to ensure the consistent application of the GDPR across the EU. The real teeth of the GDPR lie with each of the DPAs, who are empowered by national enabling legislation to supervise, monitor and enforce compliance with the new regime.

With the GDPR in place for a mere 6 months, and with no fines issued as of the date of publication, it is a little too early to pass judgment on how effective in practice the regime will be. However, the warning sirens are starting to flash: since 25 May, a number of DPAs have been inundated with complaints, with the European Data Protection Supervisor Giovanni Buttarelli noting that complaints to French and Italian supervisory authorities have risen by 53% from last year.

Some of most notable complaints in the pipeline are as follows.

Max Schrems, the notorious Austrian privacy campaigner, submitted complaints moments after the GDPR came into force against Google, Facebook, Instagram and WhatsApp

CONCERNING THEIR OBTAINING OF 'FORCED CONSENT' FROM USERS.

Investigations are in the early stages and are spread across four different supervisory authorities (France, Belgium, Hamburg (Germany) and Austria).

Ireland's Data Protection Commission is currently investigating the recent Facebook data breach that saw

HACKERS GAIN ACCESS TO NEARLY 50 MILLION ACCOUNTS.

The UK's Information Commissioner's Office (**ICO**) has begun an investigation into British Airways, following allegations that a

HACKER STOLE CREDIT CARD DATA ASSOCIATED WITH THE PURCHASE OF 380,000 AIRLINE TICKETS.

The French data protection authority has issued formal notices to two advertising start-ups relating to the

PROCESSING OF GEOLOCATION DATA

for ad targeting and mobile user consent. Both companies have been ordered to obtain their users' valid consent within 3 months or face greater sanctions.

Perhaps most relevantly, the ICO has recently issued the first official enforcement notice under the GDPR against a non-EU established company, Canadian data consultancy AggregateIQ, as part of the broader review of the

ELECTIONEERING PRACTICES RESULTING FROM THE CAMBRIDGE ANALYTICA SCANDAL.

For more information, please refer to our "GDPR: Ain't No Ocean Wide Enough" article.

WHAT DOES THE POST-GDPR WORLD LOOK LIKE?

Given the already broad scope of the GDPR and the resulting compliance measures being undertaken by organisations worldwide, analysts predict that no substantial strengthening of the regulation itself is on the horizon.

More likely are regional flow-on effects, whereby non-EU national privacy frameworks adapt with varying degrees of reference to the new standard set by the GDPR.

Driven in large part by a series of high-profile data breaches and poor data management practices being exposed, the GDPR represents a codification of a larger global movement towards prioritising personal privacy and data security. With this in mind, the more optimistic industry commentators have pointed to the fact that introducing a robust and visible GDPR compliance regime is now seen as method of competitive differentiation. Organisations that were previously expected to employ stringent physical security measures are now equally expected to have industry-leading data security measures in place – with those that fall short suffering a blow to both their reputation and bottom line.

However, the picture doesn't seem to be entirely rosy. One unintended consequence of the GDPR's incredibly strict requirements around obtaining consent is that certain companies seem to have chosen to adopt the path of 'least compliance', or as Bloomberg put it "it's easier to block half a billion people from accessing your product than comply with Europe's new GDPR". Of course, geoblocking European users is not only an imperfect means of dodging compliance, but it also makes for a more divided digital ecosystem.

Moves such as these foreshadow another trend in personal data protection: the pay-for-privacy market.

With many dominant web players preferring a data-driven business model rather than a traditional pricing system, personal information and online activities have become the 'price' paid by users. However, if both consumer demands and legislative controls seek to regulate core features of this business model, it is foreseeable that the ability to opt-out of data collection for a price will be more commonly offered. Comments from Facebook COO, Sheryl Sandberg, certainly align with this, indicating that opting out of their services tracking and analytics at the highest level would be a paid product (although it is not clear how this would work in practice, as GDPR compliance is not an 'option' for these companies).

Innovative approaches to the pay-for-privacy model are already being deployed, such as by Coil, where users pay a monthly subscription to contribute capped micropayments to affiliated content creators for the time spent on a given webpage. The hope for underlying services such as Coil is that their success will enable creators to more readily offer ad-free, privacy conscious content. As any future pay-for-privacy features will certainly exclude individuals on the basis of affordability, these shifts also underscore the fact that full personal privacy is a privilege in the digital era. When many online services have become so ubiquitous that they border on public utilities, the fairness of the pay-for-privacy model is called into question.

"IT'S EASIER TO BLOCK HALF A BILLION PEOPLE FROM ACCESSING YOUR PRODUCT THAN COMPLY WITH EUROPE'S NEW GDPR."

FOCUS: THE ePRIVACY REGULATION

While the GDPR has rightly been front of mind this year, it is worth remembering that it is only part of the EU's much larger 'digital single market' strategy. The next linchpin is the EU's ePrivacy Regulation (**ePR**), which is designed to protect the privacy of personal data contained in electronic communications.

The ePR emerged as a refresh of the current *Privacy and Communications Directive* 2002, which obliged member states to regulate electronic communications. The resulting domestic regulations, such as the UK's Personal and Electronic Communications Regulation 2003 (**PECR**), addressed a wide range of matters such as confidentiality, data retention, spam and cookies. However, with the world a much different place to how it was in 2002, the ePR looks to cast a much wider net than its predecessor.

Set to operate in tandem with the GDPR, the ePR introduces a number of key changes vis a vis its predecessor, including:

SCOPE

By regulating the electronic communications of both natural and legal persons (e.g. corporations), as well as machine-to-machine communications for a future dominated by the internet of things.

TECHNOLOGIES

By broadening the covered technologies to include not only traditional voice, text and email communications, but also newer methods such as those employed in Facebook Messenger, Instagram and WhatsApp, as well as voice activation with virtual assistants such as Amazon Alexa and Google Assistant.

EXTRA-TERRITORIAL EFFECT

By extending its reach to organisations located outside of the EU that process electronic communications data of individuals who are located in the EU.

RESTRICTIONS

By mandating that explicit and informed permission be the only condition under which a company may send electronic communications or use data about users' electronic communications, and then only for the specific, agreed-upon purpose.

SANCTIONS

By including fines of a magnitude similar to those in place under the GDPR, with maximum administrative fines up to the greater of €20,000,000 or 4% of annual global turnover.

The draft text of the new law was approved by the European Parliament in late 2017, and is currently under review by the Council of the European Union (a group of government officials representing the 28 EU Member States). While it is projected to come into effect sometime in 2019 or 2020, due to strong industry backlash consultation and reforms are ongoing.

We will keep you posted with developments as and when they arise.

SIMON BURNS
Partner
T +61 2 9263 4776
M +61 448 100 727
E sburns@gtlaw.com.au

MICHAEL CAPLAN
Partner
T +61 3 8656 3333
M +61 413 605 274
E mcaplan@gtlaw.com.au

TIM GOLE
Partner
T +61 2 9263 4077
M +61 410 540 745
E tgole@gtlaw.com.au

ANDREW HII
Partner
T +61 2 9263 4046
M +61 457 808 018
E ahii@gtlaw.com.au

SHEILA MCGREGOR
Partner
T +61 2 9263 4152
M +61 414 399 976
E smcgregor@gtlaw.com.au

LESLEY SUTTON
Partner
T +61 2 9263 4296
M +61 414 265 169
E lesutton@gtlaw.com.au

MELISSA FAI
Special Counsel
T +61 2 9263 4685
M +61 404 873 252
E mfai@gtlaw.com.au

ALBERT YUEN
Special Counsel
T +61 3 8656 3316
M +61 412 023 032
E ayuen@gtlaw.com.au

NIKHIL SHAH
Consultant
T +61 2 9263 4048
E nshah@gtlaw.com.au

EDWARD DAVIDSON
Lawyer
T +61 2 9263 4610
E edavidson@gtlaw.com.au

GILBERT +TOBIN

SYDNEY
Level 35 International Towers Sydney
200 Barangaroo Avenue
Barangaroo NSW 2000
Australia
T +61 2 9263 4000
F +61 2 9263 4111

MELBOURNE
Level 22
101 Collins Street
Melbourne VIC 3000
Australia
T +61 3 8656 3300
F +61 3 8656 3400

PERTH
Level 16 Brookfield Place Tower 2
123 St Georges Terrace
Perth WA 6000
Australia
T +61 8 9413 8400
F +61 8 9413 8444

GTLAW.COM.AU