Should we be worried?

The impact of the Google GDPR decision for Australian and New Zealand companies

LexisNexis®

Google has been fined €50 million by the French data protection agency, Commission Nationale de l'Informatique et des Liberts (CNIL).[i] Whilst the penalty likely caused more than a sharp intake of breath from Google executives, it would have also caused heartburn for a number of its competitors such as Facebook, LinkedIn and Amazon.

But what impact does such a decision have for Australian and New Zealand companies?

To briefly recap....

On 21 January 2019 the CNIL finally brought its decision down in relation to Google LLC's (**Google**) alleged failure to comply with the General Data Protection Regulation (**GDPR**). The case was a number of months in the making after claims were initially brought on 25 May 2018, the day the GDPR commenced.

Of particular note is the fact that the French agency imposed the largest fine to date for failure to comply with the GDPR. Specifically, Google was penalised for:

- a failure to comply with the GDPR requirements to provide transparent information to data subjects via its Android operating system; and
- having no legal basis (as required under Article 6) for processing personal data in respect of its personalised ad function.

At €50 million, the fine is considerable and makes it very clear the seriousness with which GDPR compliance will be regarded (at least by the French data protection authority). Google has promised it will be challenging the fine.

Now that the dust has settled, what happened, why is it important and should local companies be worried?

> *At €50 million, the fine is considerable and makes it very clear the seriousness with which GDPR compliance will be regarded.*

Some initial takeaways

For Australian and New Zealand companies keen to ensure they are managing privacy risks properly, there are a few tips to take on board:

- Confirm whether your organisation is first required to comply with the privacy obligations set out in the Privacy Act, 1988 (Cth) or the New Zealand Privacy Act, 1993 (**Privacy Act**). Whilst there are a number of exceptions for smaller businesses in particular, many commercial activities involving the use of personal information will see your organisation come back within the scope of the Privacy Act;

- If your organisation is required to comply with the Privacy Act, are they also required to comply with the General Data Protection Regulation (**GDPR**)? We discuss some of the important jurisdictional threshold issues below;

- Finally, there is clearly a regulatory trend towards greater levels of privacy compliance and enforcement as evidenced by the recently announced additional funding for the Office of the Australian Information Commissioner (OAIC) as well as proposed increased penalties. With such changes afoot your organisation will benefit from improving privacy compliance across its business operations now.

Background

On 25 May 2018 and 28 May 2018, CNIL received two separate collective complaints from the privacy rights groups None Of Your Business ("NOYB") and La Quadrature du Net ("LQDN"), claiming that Google did not have a valid legal basis to process personal data of its service users.

The complaints specifically concerned the use of personalised ads on smart phone devices using the Android operating system with a user's Google account. The French authority determined Google had breached the GDPR in two separate ways. First, a lack of transparency, and second a lack of valid consent regarding the targeted ads. We look at each in turn.

Lack of transparency

Transparency is one of the key features of the GDPR and must be effectively incorporated across all data processing activities.

The regulator considered the process a user was required to go through when signing up for a Google account. Critical information relating to the processing purposes, data storage periods and the categories of personal data collected were found to be inaccessible and when included only available across multiple documents. Users had to undertake a number of steps before being able to access the information and when they did locate it, much of it was unclear. Obtaining relevant information relating to personalization of ads was a 5 step process and for geo-tracking 6 steps were required.

When considering Google's processing activities, the CNIL closely looked at the scale of Google's service offering. The large number of services available including Google's primary search function, YouTube media, Google home, Google maps, Playstore and Google pictures all required "massive and intrusive" amounts of data processing. The CNIL found at least 20 services on offer which whilst extensive is not unusual when compared with similar offerings by other technology platforms.

> *Transparency is one of the key features of the GDPR and must be effectively incorporated across all data processing activities.*

However, the regulator found Google's description of the processing activities required in relation to these broad range of services as being "too generic and vague". Similarly, the information communicated was not clear enough so that a user could understand that the legal basis of processing operations for the ads personalization was user consent, and not the legitimate interest of the company. Finally, the CNIL found that there was no information provided in relation to the applicable data retention periods.

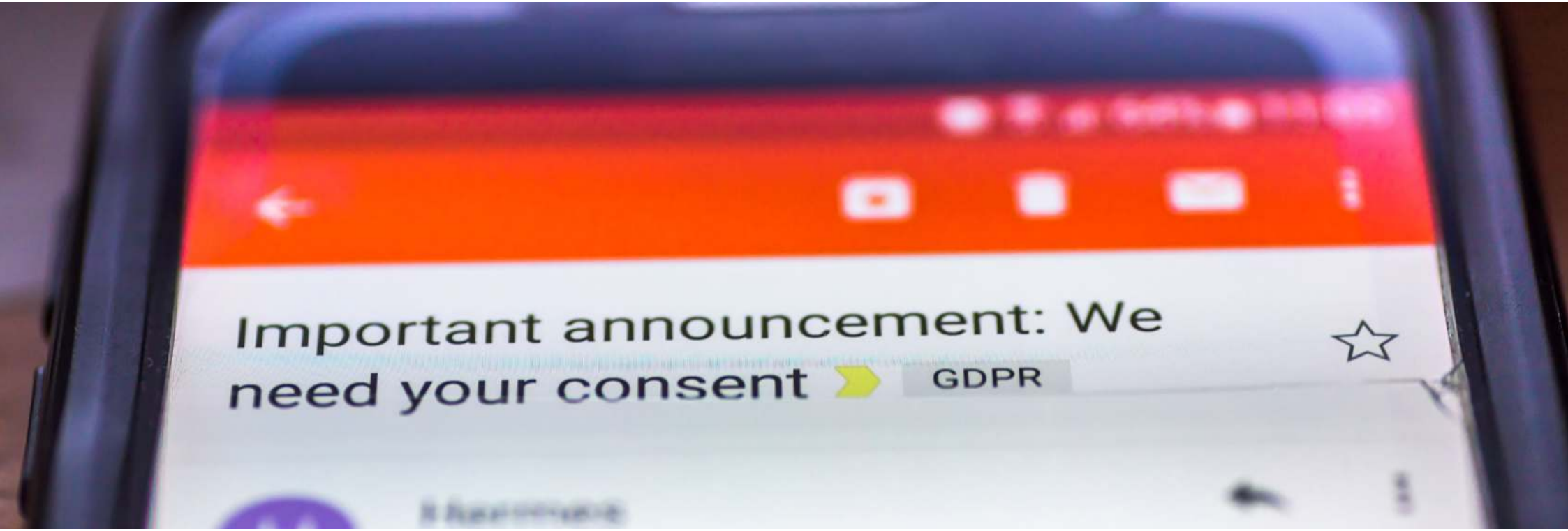
All of this combined resulted in the CNIL finding there was a general violation of the GDPR requirement that relevant information should be "easily accessible" to users.

No valid consent obtained

The regulator also found Google has not validly obtained users' consent to process data for ads personalisation. It was found that users were unable to give informed consent as the information provided did not adequately describe the broad extent of data being collected and processed in relation to the services.

The CNIL also found that users were unable to give "unambiguous" and "specific" consent. Boxes relating to ad personalisation were already pre-ticked as a default position during signup. Users could complete the application without being able to positively agree to the specific types of processing required for each service offering. The GDPR with its strict requirement that consent could only be given for a specific processing activity was not met by this "catchall" approval process.

The CNIL was looking for there to be some "clear affirmative action from the user" to effectively meet the consent requirements outlined under the GDPR. They gave the option of a user being able to tick a non pre-ticked box as an example. Unfortunately for Google their signup process did not meet this requirement.



Penalty

The regulator imposed a €50 million fine on Google and cited Google's failure to meet the essential principles of the GDPR around transparency and consent. The fact that the breaches were not one-off occurrences was also taken into account as was Google's deep market penetration.

Whilst the decision has clear implications for EU based organisations what are the likely implications for Australian or New Zealand companies?

When does the GDPR apply to Australian or New Zealand organisations?

The answer depends on whether the GDPR extends to the locally based company or not.

For those companies solely required to comply with the Australian Privacy Act, 1988 or NZ Privacy Act, 1993 (**Privacy Act**) the likely reality is the decision, whilst informative, only provides a timely reminder of the importance of managing privacy rights of individuals, particularly in a time when technology innovation allows organisations to reach in and grab large volumes of personal data from unsuspecting users.

Such organisations who have to comply with the Privacy Act would be well served to review their data collection activities and ensure they meet or exceed the privacy principles outlined in the local Privacy act. As to the risk of incurring similar penalties from the Australian regulator, the risks are presently low. That said, there are proposed changes on the horizon which we discuss in more detail below.

For those organisations that are required to comply with the GDPR the position is a little different.

Before commenting on the risks brought about by this decision, it is worth recapping on the extension of the GDPR to local companies.

Organisations that have to comply with the Privacy Act - otherwise known as APP entities, may need to comply with the GDPR if:

- They have an establishment in the EU. i.e. a physical location in the EU;
- In the event that they do not have an establishment in the EU, they:
  - Offer goods or services in the EU (even where no payment is required); or
  - Monitor the behaviour of individuals in the EU.

Organisations that have a physical establishment, such as an office, in the EU and process personal information will need to ensure that they comply with the GDPR even if the data is not processed in the EU.

Examples of Australian and New Zealand organisations that do not have an establishment in the EU but may still be required to comply with the GDPR include organisations that have:

- A website that allows payment for goods or services to be made in Euros;
- A website that allows visitors to the website to choose to view the website in the language of any of the EU member nations, provided that it is possible to ascertain that the Australian and/or NZ business intended to offer goods and services to individuals in the EU; and
- Technology that enables it to track individuals in the EU online and profile the individuals to analyse or predict the individuals' behaviours, attitudes and preferences. This may include social network share buttons that can not only track online browsing habits but are tied to social network accounts.

Clearly, an Australian and/or NZ business with a physical presence in the EU will be captured, but so too will businesses operating out of Australia and/or NZ who use a website to sell goods or services to customers located in the EU.

Even those businesses that do not necessarily sell goods or services but reference EU customers or users in the EU or track or monitor the behaviour of individuals using cookie or similar technologies may fall within scope.

This article does not seek to go into the specific compliance requirements for those organisations that fall within the GDPR obligations. Suffice to say if your company is within scope you will likely have a laundry list of compliance obligations depending on the nature of your organisation's activities. Clearly those with a physical presence in the EU such as Google will have a longer "to do" list than those headquartered out of Australia and/or NZ with only a limited exposure to the EU.

We do need to comply with GDPR but do we really need to worry?

Since the introduction of the GDPR in May 2018, there have been 59,000 personal data breaches notified to supervisory authorities in the EU. Of these notifications, there have been 91 reported fines. With the exception of this latest fine against Google (which was in respect of a broader breach of the GDPR rather than a personal data breach), most fines to date are relatively low in value.

The EU supervisory authorities including the CNIL in France will likely continue to have their sights firmly set on the big players as they respond to actual complaints made in the EU. Organisations such as NOYB will also continue to focus their attentions on big tech from a privacy perspective.

Whilst this does not mean Australian and/or NZ based companies subject to the GDPR should breathe a sigh of relief - it does mean the focus for their compliance should effectively extend to improved privacy practices in relation to their EU operations in particular.

In Australia we have seen what appears to be a slightly higher standard of compliance required of technology companies in decisions such as the long running Ben Grubb group of cases but nothing like the attention Facebook, Google, and others are receiving in the EU and US. Facebook in particular has attracted the ire of regulators with a recent decision of the German Federal Cartel Office (FCO, *Bundeskartellamt*), finding that the way Facebook collects data from various sources and merges it with its user profiles is a breach of the GDPR and, at the same time, an abuse of a dominant position. More to come on this recent decision in due course.[ii]

> *"Since the introduction of the GDPR in May 2018, there have been 59,000 personal data breaches notified to supervisory authorities in the EU."*

OK, so what should we be doing differently then?

The Google decision should serve as a wake-up call for companies who collect, manage and store personal information both in Australia and/or New Zealand under the Privacy Act and overseas under the watchful eye of the GDPR.

Local privacy laws and the GDPR are both focused on protecting the privacy rights of individuals. Both regimes are firmly based on "privacy by design" principles which encourage transparency and accountability regarding information handling practices.

So if your company is processing personal information or personal data as it is referred to in the EU it needs to ensure it does so in a transparent and easy to follow way.

It is therefore critical to ensure adequate information is provided to users setting out the service description, what information is being collected and how, how it is being used/processed or disclosed and to whom, where it is being stored and for how long.

> *The Google decision should serve as a wake-up call for companies who collect, manage and store personal information both in Australia and/or New Zealand under the Privacy Act and overseas under the watchful eye of the GDPR.*

Avoid using vague or general statements - be specific about your data processing activities and relate them back to the specific service. Consider including an FAQ section as part of the conversation you have with your users. This may assist you to provide the necessary details in an informative and clear way. Don't bury important information about privacy rights in the fine print - include it up front and alongside details of the data processing activity if at all possible.

For those companies subject to GDPR, make sure you understand and ensure the legal basis for processing is clearly articulated. If you choose to rely on consent, ensure the process and language used meets the particular requirements for valid consent. You may also consider whether a separate legal basis for processing may be a better alternative and easier to implement.

Many privacy policies and collection notices once drafted sit idly on a website never to be reviewed much less revised. They include well intentioned rights and obligations which are never properly rolled out across the business. Effective privacy compliance requires companies to adopt the "privacy by design" approach. Make it part and parcel of how you do business and ensure it forms a key part of the culture of your organization.

“Effective privacy compliance requires companies to adopt the “privacy by design” approach. Make it part and parcel of how you do business and ensure it forms a key part of the culture of your organization.”

Final comments and wrap up

The Google decision poses immediate implications for businesses required to comply with the GDPR. It does have implications more broadly for Australian and New Zealand companies too. It is a clear signal to companies who collect, manage and use personal information that the privacy rights of individuals are to be protected.

In Australia, it seems the Federal Government is also watching such developments carefully. On 25 March 2019, the Government threatened to 'punish those firms and platforms who defy our norms and values' in announcing a number of proposed amendments to the Privacy Act including:

- Increased penalties for all entities covered by the Privacy Act, from the current maximum penalty of $2.1 million for a company) to the higher of:
  - $10 million;
  - Three times the value of the benefit obtained from the breach; or
  - 10% of the company's annual domestic turnover in the last 12 months.
- New infringement notice powers for the OAIC backed by new penalties of up to $63,000 for bodies corporate for failure to cooperate with efforts to resolve minor breaches;
- Power for the OAIC to publish prominent notices about specific breaches and ensure those directly affected are advised;
- A requirement for social media and online platforms to stop using or disclosing an individual's personal information upon request; and
- A resulting code for social media and online platforms which trade in personal information.

It is the proposed "turnover" penalty which has grabbed the headlines as it starts to resemble the GDPR-like penalties we currently see in place in the EU. It remains to be seen whether the proposed changes in Australia will be implemented as drafted after the Federal election which occurred in May 2019. Irrespective of what may or may not happen post-election, clearly a regulatory shift is occurring within Australia. Best assist your organization to meet that challenge now and ensure privacy rights form a key element of how you do business moving forward.

i https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc
ii https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html

About the Author

Dudley Kneller
Partner | Madgwicks Lawyers

Dudley Kneller is a technology lawyer with a speciality in privacy, cyber risk and strategic sourcing and supply projects. He has more than 20 years' experience practising across Australia, Europe and the UK, and has worked on projects based in a range of countries, including the Philippines, India, Russia and throughout South America.

Dudley is listed in Best Lawyers in Australia for Information Technology Law 2020. He is also listed as one of a group of recommended Technology, Media, Telecommunications Lawyers for Melbourne in Doyle's Guide from 2015-2019.

T: +61 3 9242 4730
E: dudley.kneller@madgwicks.com.au

About LexisNexis®

LexisNexis Legal & Professional is a leading global provider of legal, regulatory and business information and analytics that help customers increase productivity, improve decision-making and outcomes and advance the rule of law around the world. As a digital pioneer, the company was the first to bring legal and business information online with its Lexis® and Nexis® services.

LexisNexis Legal & Professional, which serves customers in more than 130 countries with 10,000 employees worldwide, is part of RELX Group, a global provider of information and analytics for professional and business customers across industries.

LexisNexis is supporting the Australian Human Rights Commission as a project partner in a landmark inquiry into the challenges to our rights and freedoms presented by technologies such as artificial intelligence, social media, and big data.

The AI-powered Lexis Advance platform uses machine learning and natural language processing technology to deliver a research experience like no other.

LexisNexis also delivers a range of subscription and custom analytics solutions for the tech-driven lawyer.

For more information, **visit our website**.

NA052019CC