

The General Data Protection Regulation – Another Key Compliance Area for Global Business

By: Colin Loveday and Richard Abraham



Colin Loveday is a Partner in the Commercial Litigation team in the Sydney office of Clayton Utz.

Richard Abraham is a Senior Associate in Colin's team at Clayton Utz.¹



ON May 25, 2018, the European Union implemented the General Data Protection Regulation (the “GDPR”).² The GDPR, which replaces the 1995

Data Protection Directive, will apply in each EU member state, regulating the processing of personal data without the need for national implementation.³ The

¹ The authors would like to thank Alexandra Wedutenko and Mathew Baldwin of Clayton Utz whose work on the GDPR they have drawn upon in the preparation of this paper, see Alexandra Wedutenko and Mathew Baldwin, *Australian organisations beware – you could be caught by EU's new General Data Protection Regulation*, February 1, 2018, available at <https://www.claytonutz.com/knowledge/2018/february/australian-organizations-beware-you-could-be->

[caught-by-eus-new-general-data-protection-regulation](#).

² Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, available at http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf.

³ Although the UK is set to leave the EU in March 2019, the UK Government has said it expects the GDPR will continue to apply

scope of processing is defined broadly to mean the operations performed on personal data, including collection, storage, alteration, use and disclosure (hereinafter “Processing”).

EU members will supplement the GDPR with their own laws, including laws that identify the relevant national supervisory bodies. The GDPR will grant individuals the ability to take direct action for infringement, and national supervisory bodies the right to levy significant fines against companies that breach it. Importantly, the GDPR will apply to organizations without an EU establishment if Processing of personal data is related to either:

- (a) offering goods or services to data subjects in the EU; or
- (b) monitoring data subjects' behavior as far as it takes place in the EU.

The potential impact of the implementation of the GDPR not only within the EU, but for those organizations who do business with, or deal with information

concerning, EU citizens and businesses is readily apparent.

Like data protection, anti-bribery and corruption is a current focus of regulators, politicians and the press. An organization's exposure to risk in both of these areas will increase together with their involvement in the global economy - indeed, even greater degrees of globalization are only made possible by rapidly increasing developments in technology - and the capacity to process enormous quantities of data instantaneously.

There are further similarities: an attempt at uniformity of regulation, an expansive approach to jurisdiction, and the potential for large fines for contravention.

Therefore, while at first anti-bribery legislation and the GDPR may appear to be strange bedfellows, the nature and potential impact of the GDPR gives rise to some apparent parallels. One thing is certain, both are going to be areas of considerable focus for legal and compliance personnel in the coming years.

This paper provides a short refresher of key provisions of the Foreign Corrupt Practices Act,⁴ looks at how similar (but not identical) legislation has been

in substance via the recently tabled Data Protection Bill, *see* Department for Digital, Culture, Media & Sport, *Data Protection Bill: Fact Sheet-overview*, March 5, 2018, available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/fil

e/685647/2018-03-05_Factsheet01_Bill_overview.pdf.

⁴ This refresher is provided from an Australian perspective, and the authors do not profess to have more than a limited understanding of the FCPA.

enacted in other jurisdictions, and in particular how the enforcement of similar laws has occurred across various jurisdictions. We then discuss some of the key provisions of the GDPR and consider what lessons may be drawn from the development and enforcement of FCPA-style provisions when considering the potential impact of the GDPR.

I. Anti-Bribery and Corruption Regulation

A. Setting the Benchmark - the FCPA

The Foreign Corrupt Practices Act of 1977⁵ was enacted for the purpose of making it unlawful for certain classes of persons and entities to make payments to foreign government officials to assist in obtaining or retaining business. As is well understood, for present purposes there are two broad offenses under the FCPA:

- **the anti-bribery provisions:** Under the FCPA, it is a criminal offense to make a payment or offer payment to a foreign official for the purposes of obtaining business for any person; and

- **the 'books and records' provisions:** the FCPA also requires companies whose securities are listed in the United States to meet the so-called "books and records" accounting provisions. These were designed to work in tandem with the anti-bribery provisions and require corporations covered by the provisions to (a) make and keep books and records that accurately and fairly reflect the transactions of the corporation; and (b) devise and maintain an adequate system of internal accounting controls.

A convenient guide on the ins and outs of the FCPA is the detailed joint guidance first published by the Department of Justice and Securities and Exchange Commission in November 2012 - the *Resource Guide to the U.S. Foreign Corrupt Practices Act*.⁶

The anti-bribery provisions of the FCPA originally applied to all U.S. persons and certain foreign issuers of securities. However following amendments in 1998, the anti-bribery provisions now also

⁵ As amended, 15 U.S.C. §§ 78dd-1, et seq. (the "FCPA").

⁶ Available at <https://www.justice.gov/criminal-fraud/fcpa-guidance>.

apply to foreign firms and persons who cause, directly or through agents, an act in furtherance of such a corrupt payment to take place within the territory of the United States. The DOJ takes an expansive approach to jurisdiction - an approach has been mirrored more recently in the legislation and prosecutorial approach in other countries.

1. Recent Developments Concerning Investigation and Enforcement

Just as the DOJ takes an expansive approach to jurisdiction, it also takes a "global", rather than "local" approach to investigation and enforcement. The rationale for such an approach was recently articulated by Deputy U.S. Attorney General Rosenstein:

Foreign Corrupt Practices Act enforcement focuses on the global marketplace, because the world is interconnected. Economic problems in distant places

affect American businesses and financial markets. So too does foreign corruption.⁷

This has translated in practice to increased international cooperation. For example, when discussing a recent DOJ enforcement action Deputy U.S. Attorney General Rosenstein confirmed that the DOJ had cooperated with enforcement authorities in the UK, Brazil, Austria, Germany, the Netherlands, Singapore and Turkey, and noted that the DOJ looked forward to continued international cooperation.⁸ This move to increased cooperation is supported by 2016 figures, which showed that more than 40% of the resolutions in U.S. foreign bribery cases involved cooperation with foreign law enforcement agencies.⁹

The involvement of multiple regulatory authorities (both within and across different jurisdictions) gives rise to the potential that an organization may face multiple enforcement actions in respect of

⁷ Remarks at the American Conference Institute's 20th Anniversary New York Conference on the Foreign Corrupt Practices Act. Available at <https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-american-conference-institutes>.

⁸ See Department of Justice, Press Release, *Deputy Attorney General Rosenstein Delivers Remarks at the 34th International Conference on the Foreign Corrupt Practices*

Act, November 29, 2017, available at <https://www.justice.gov/opa/speech/deputy-attorney-general-rosenstein-delivers-remarks-34th-international-conference-foreign>.

⁹ See OECD, *Data on enforcement of the Anti-Bribery Convention*, available at <http://www.oecd.org/daf/anti-bribery/data-on-enforcement-of-the-anti-bribery-convention.htm>.

the same conduct - or to adopt the sporting analogy used by the Deputy Attorney General - regulators "piling on" a tackled player.¹⁰

In recognition of this, in May 2018 the DOJ announced a new departmental policy which instructs Department components to appropriately coordinate with one another and with other enforcement agencies in imposing multiple penalties on a company for the same conduct. The policy has four core features. For present purposes, the most important is the encouragement of Departmental attorneys, when possible, to coordinate with other federal, state, local, or foreign enforcement authorities seeking to resolve a case with a company for the same misconduct.

In announcing the new policy, the Deputy Attorney General sounded a warning to those who may wish to seek to "game" the new policy:

Cooperating with a different agency or a foreign government is not a substitute for cooperating with the Department of Justice. And we will not look kindly on companies that come to us

after making inadequate disclosures to secure lenient penalties with other agencies or foreign governments. In those instances, the Department will act without hesitation to fully vindicate the interests of the United States.¹¹

2. Enforcement Record

The FCPA celebrated its fortieth birthday in 2017. While perhaps an underachiever in childhood and into its teenage years, it has racked up an impressive resume of enforcement actions and sanctions:¹²

- a total of 537 enforcement actions have been brought (208 by the SEC and 329 by the DOJ);
- of these, the vast majority have been settled (92.58% of defendants settle with the SEC and 76.1% of defendants settle with the DOJ); and
- \$11,642,712,053 in monetary sanctions have been imposed in all FCPA-related enforcement actions.

¹⁰ *Supra*, note 7.

¹¹ *Id.*

¹² All figures taken from the Stanford Law School, *Foreign Corrupt Practices*

Clearinghouse, available at <http://fcpa.stanford.edu/statistics-keys.html> (statistics as of last visit on June 22, 2018).

The billions of dollars in corporate sanctions and fines often dominate the headlines, but the DOJ is focused on the investigation and prosecution of individuals for FCPA offenses. The U.S. Deputy Attorney General observed in November 2017 that a total of 19 individuals had pleaded guilty or been convicted in FCPA-related cases that year, and used the point to somewhat ominously illustrate that:

Effective deterrence of corporate corruption requires prosecution of culpable individuals. We should not just announce large corporate fines and celebrate penalizing shareholders.¹³

Sometimes, prosecutorial focus will shift from the corporation and its executives to those who advise them. In 2010, the DOJ announced personal charges against the attorney for a major pharmaceutical company alleging obstructing an official proceeding, concealing and falsifying documents to influence a federal agency, and making false

statements. The conduct occurred in the context of a Food and Drug Administration into off-label promotion of a pharmaceutical product.¹⁴ The attorney was acquitted under Federal Rule of Criminal Procedure 29 on the grounds that the government had failed to present evidence sufficient to prove any of the counts beyond a reasonable doubt.¹⁵ In its judgment, the Court stated:

A lawyer should never fear prosecution because of advice that he or she has given to a client who consults him or her, and a client should never fear that its confidences will be divulged unless its purpose in consulting the lawyer was for the purpose of committing a crime or a fraud.

There is an enormous potential for abuse in allowing prosecution of an attorney for the giving of legal advice.¹⁶

¹³ See Department of Justice, Press Release, *supra* note 8. As at May 2018, the DOJ FCPA Unit had announced 8 guilty pleas since the start of 2018, *see* Rosenstein Speech, *supra* note 7.

¹⁴ See Department of Justice, Press Release, *Pharmaceutical Company Lawyer Charged with Obstruction and Making False Statements*, Nov. 9, 2010, available at

https://www.justice.gov/sites/default/files/civil/legacy/2014/01/09/DOJ_Press_release_11-9-10.pdf.

¹⁵ *United States v. Stevens*, No. 10-694 (D. Md. May 10, 2011).

¹⁶ *Id.* available at https://jenner.com/system/assets/assets/165/original/United_States_v._Stevens.pdf?1314198465.

As an aside, while the attorney was successful in the defense of the individual charges, eventually the company agreed to pay \$3 billion to settle the corporate proceedings.¹⁷

B. The Rising Tide of Regulation - OECD Convention, the UK and Australia

1. OECD Convention

Like the U.S., Australia is a signatory to the Organization for Economic Co-operation and Development (“OECD”) *Convention on Combating Bribery of Foreign Public Officials in International Business Transactions* (the “OECD Convention”). The OECD Convention requires signatories to criminalize bribery of foreign public officials in international business transactions and implement a range of related measures to make this criminalization effective.

There are currently 35 OECD countries and 8 non-OECD countries who are signatories to the OECD Conventions – and this list is increasing. The coalescence of global business practices and technology (which could see a

nexus with a particular jurisdiction established in unusual and unexpected ways), together with an increasing number of jurisdictions enacting anti-bribery legislation and aggressive approaches to jurisdiction taken by enforcement agencies in a number of these jurisdictions mean that anti-bribery and corruptions needs to remain top of mind for corporate compliance.

To illustrate the point, in its December 2017 publication *Fighting the Crime of Foreign Bribery*,¹⁸ the OECD noted:

- foreign bribery is a crime in all 43 parties to the OECD Convention;
- in the period between 1999 and the end of 2016, 443 individuals and 158 entities have been sanctioned under criminal proceedings for foreign bribery in 20 countries which are parties to the OECD Convention (while 23 countries had yet to conclude a foreign bribery enforcement action);
- 500 investigations were ongoing in 29 countries; and

¹⁷ See Katie Thomas and Michael S. Schmidt, *Glaxo Agrees to Pay \$3 Billion in Fraud Settlement*, NY TIMES, July 2, 2012, available at <http://www.nytimes.com/2012/07/03/business/glaxosmithkline-agrees-to-pay-3-billion-in-fraud-settlement.html>.

¹⁸ OECD, *Fighting the Crime of Foreign Bribery*, 2017, available at <http://www.oecd.org/corruption/Fighting-the-crime-of-foreign-bribery.pdf>.

- 125 individuals and 19 entities were subject to prosecution in 11 countries for offenses under the OECD Convention.

2. UK

The UK Bribery Act 2010 (“Bribery Act”) was introduced with considerable fanfare in 2011. One significant difference between the FCPA and the Bribery Act was the introduction of a “failure to prevent bribery” offense. Under Section 7 of the Bribery Act, a commercial organization is guilty of failure to prevent bribery if a person associated with the commercial organization bribes another person intending:

- (a) to obtain or retain business for the commercial organization, or
- (b) to obtain or retain an advantage in the conduct of business for the commercial organization.

It does not matter if the associated person is a British citizen who could be prosecuted for the offense or not, meaning that a

company with a jurisdictional link to the UK could be prosecuted for something that a non-British citizen did outside the UK.

If the commercial organization can prove that it had in place “adequate procedures” designed to prevent persons associated with it from committing these acts, then it has a defense to the charge. The UK Ministry of Justice has published guidance that addresses what might constitute adequate procedures.¹⁹

Following the introduction of the Bribery Act, there was a period where Section 7 remained untested. This changed when the Serious Fraud Office (“SFO”) entered into its first Deferred Prosecution Agreement (“DPA”) in respect of the offense under Section 7 in November 2015 (ICBC Standard Bank Plc), and achieved its first conviction in February 2016 when a construction and professional services company (Sweett Group PLC) was sentenced and ordered to pay £2.25 million as a result of a conviction arising from a SFO investigation into the activities of one of Sweett Group’s subsidiaries in the United Arab Emirates. In sentencing, the Court observed:

The whole point of section 7 is to impose a duty on those running such companies

¹⁹ Rt. Hon. Nick Herbert, Ministry of Justice, *Bribery Act 2010 guidance*, February 11, 2012, available at <https://www.gov.uk/>

government/publications/bribery-act-2010-guidance.

*throughout the world properly to supervise them. Rogue elements can only operate in this way – and operate for so long – because of a failure properly to supervise what they are doing and the way they are doing it.*²⁰

More recently, the SFO entered into a DPA with Rolls-Royce PLC, which involved the payment of £497.25 million (plus the SFO's costs in the amount of £19 million).

This was the highest-ever enforcement action against company in the UK for criminal conduct and was reached in circumstances where Rolls-Royce PLC fully cooperated in the investigation and introduced a program of corporate reform and compliance.²¹ Importantly, the DPA did not prevent further investigation into the conduct of

individuals, and indeed Rolls-Royce PLC agreed as a condition of the DPA to cooperate with any future prosecution of individuals. Similar agreements have been announced between Rolls-Royce PLC and authorities in the U.S. and Brazil.

Finally, February 2018 saw a ruling in the first contested prosecution of the offense under section 7 of the Bribery Act when Skansen Interior Limited was found guilty of failing to prevent bribery. Following this decision, two directors of the parties involved (including the former managing director of Skansen Interior Limited) were jailed after pleading guilty to bribery.²²

3. Australia

Australia ratified the OECD Convention in 1999. Australia is also a party to the United Nations Convention against Corruption

²⁰ See Serious Fraud Office, News Release, *Sweett Group PLC sentenced and ordered to pay £2.25 million after Bribery Act conviction*, February 19, 2016, available at <https://www.sfo.gov.uk/2016/02/19/sweett-group-plc-sentenced-and-ordered-to-pay-2-3-million-after-bribery-act-conviction/>.

²¹ See Serious Fraud Office, News Release, *SFO completes £497.25m Deferred Prosecution Agreement with Rolls-Royce PLC*, January 7, 2017, available at <https://www.sfo.gov.uk/2017/01/17/sfo-completes-497-25m-deferred-prosecution-agreement-rolls-royce-plc/>. The SFO press release explains: "The indictment, which has been suspended for the term of the

DPA, covers 12 counts of conspiracy to corrupt, false accounting and failure to prevent bribery. The conduct spans three decades and involves Rolls-Royce's Civil Aerospace and Defence Aerospace businesses and its former Energy business and relates to the sale of aero engines, energy systems and related services. The conduct covered by the UK DPA took place across seven jurisdictions: Indonesia, Thailand, India, Russia, Nigeria, China and Malaysia."

²² See *Company directors jailed for bribery*, CPS, April 23, 2018, available at <https://www.cps.gov.uk/cps/news/company-directors-jailed-bribery>.

("UNCAC") of 2003. Both treaties require state parties to criminalize bribery of foreign public officials in the course of international business. Australia has given effect to its treaty obligations in Division 70 of the Criminal Code Act 1995 (Cth) (the "Criminal Code"). Section 70.2(1) makes it an offense to provide, offer or promise to provide a benefit not legitimately due to another person, with the intention of influencing the exercise of a foreign public official's duties in order to obtain or retain business or a business advantage. The terms "foreign public official" and "benefit" are both broadly defined, and the offense captures bribes made to foreign public officials either directly or indirectly via an agent, relative or business partner. Unlike the UK, Australia retains the "facilitation payment" defense.

The legislation prescribes maximum penalties for individuals of up to 10 years imprisonment and fines of up to AUD\$2.1, and for corporations, the maximum penalties are the greater of:

- AUD\$21 million (USD\$16 million, EUR€13.2 million) fine;
- three times the total benefit obtained from the bribe; or

- 10% of the company's annual turnover.

In addition to criminal penalties, any benefits obtained by foreign bribery may be forfeited to the Australian government under the *Proceeds of Crime Act 2002* (Cth). That Act establishes a regime that allows proceeds of Federal-indictable offenses to be traced, restrained and confiscated by a court. It also confers power on a court to order that a person appear before it to demonstrate that unexplained wealth was acquired by lawful means.

In recent years there has been considerable change to the anti-bribery landscape through the enactment (or proposed enactment) of new anti-bribery legislation and progress in the enforcement of such legislation.

In March 2016, the foreign bribery offense was supplemented by "books and records" style accounting offenses. The two new offenses criminalize both intentional and reckless false dealing with accounting documents.²³ The prescribed penalties for intentional false dealing with accounting documents are the same as for the foreign bribery offense, while those penalties are halved for the offense of reckless false dealing.

²³ See Division 490 of the *Criminal Code Act 1995* (Cth).

In December 2017, the Australian Government introduced further legislation into parliament which, among amendments which "aim of removing undue impediments to successful investigation and prosecution of foreign bribery offending",²⁴ seeks to introduce a new offense of failure of a body corporate to prevent foreign bribery by an associate, and a deferred prosecution agreement scheme (which would apply not only to foreign bribery, but also to other corporate offenses).²⁵ Like the UK Bribery Act, the offense of failure to prevent bribery would not apply if the body corporate can establish that they had "adequate procedures" designed to prevent the commission of the foreign bribery offense by its associates. What will constitute "adequate procedures" is not defined in the legislation. Instead, the Minister will be required to publish guidance on the steps that a body corporate can take to prevent an associate from bribing foreign public officials.

The importance of whistleblowing to the detection of corrupt conduct was acknowledged by the in a recent Australian

decision (discussed below), where the Judge observed:

I infer that the offence is difficult to detect. None of the parties to a conspiracy to bribe has an interest in its disclosure. The victim is the nation state whose foreign public officials are to receive a benefit. Absent telephone interception or a whistle-blower, it is difficult to discern how it could be detected.²⁶

It is noteworthy that the Australian Government has introduced legislation, which will, if passed, significantly bolster the requirements on publicly-listed companies and large private companies to put whistleblower policies in place, and the protections and remedies afforded to whistleblowers in certain circumstances.²⁷ Interestingly, the bill does not seek to introduce a U.S.-style "bounty" system to reward whistleblowing, but rather focuses on compensating whistleblowers who suffer loss or damage after blowing the whistle,

²⁴ Explanatory Memoranda to the *Crimes Legislation Amendment (Combatting Corporate Crime) Bill 2017* at [5], available at http://parlinfo.aph.gov.au/parlinfo/download/legislation/ems/s1108_ems_2e5f7d3d-d612-4188-ad38-ccfda42947ce/upload_pdf/655326em.pdf;fileType=application%2Fpdf.

²⁵ *Id.* at [5] and [9].

²⁶ *R v. Jousif; R v. I Elomar, R v. M Elomar*, [2017] NSWSC 1299 at [269] per Adamson J, available at <https://www.caselaw.nsw.gov.au/decision/59cad2c0e4b074a7c6e18f96>.

²⁷ See *Treasury Laws Amendment (Enhancing Whistleblower Protections) Bill 2017*.

and otherwise avoiding or punishing reprisals.

4. Enforcement Record

As of December 2017, authorities in Australia had secured seven convictions in two cases and were conducting 19 ongoing investigations - nowhere near the numbers achieved in other jurisdictions. Indeed, this has not gone unnoticed by the OECD Working Group on Bribery, which observed: "In view of the level of exports and outward investment by Australian companies in jurisdictions and sectors at high risk for corruption, Australia must continue to increase its level of enforcement."²⁸

In September 2017, three individuals who attempted to bribe a foreign official in Iraq with an amount of approximately AUD\$1million to improve the chances of their company in obtaining a construction contract valued at up to AUD\$500 million were sentenced to four years imprisonment. Two of the individuals were also fined AUD\$250,000.²⁹

We will be monitoring enforcement activity in Australia in the coming years should the

legislation currently before Federal parliament pass. The pending legislation addresses a number of elements of the offense which enforcement authorities have complained prevent effective enforcement action, and the legislation would add Deferred Prosecution Agreements to the enforcement authorities' toolkit.

II. The GDPR

An in-depth review of the provisions of the GDPR is outside the scope of this paper. However, by way of high level overview, personal data is defined under the GDPR to mean any information "relating to" an identified or identifiable natural person (a "Data Subject"). The GDPR regulates the Processing of personal data under a broad set of principles and grants privacy rights directly to data subjects.

The GDPR regulates data Processing activities by entities that determine the purpose and means by which personal data is Processed ("Controllers") and also by entities that Process personal data on behalf of Controllers ("Processors").

Obligations on Controllers and Processors under the GDPR include requirements to:

²⁸ See OECD, *Australia takes major steps to combat foreign bribery, but OECD wants to see more enforcement*, December 19, 2017, available at [http://www.oecd.org/corruption/australia-takes-major-steps-to-](http://www.oecd.org/corruption/australia-takes-major-steps-to-combat-foreign-bribery-but-oecd-wants-to-see-more-enforcement.htm)

[combat-foreign-bribery-but-oecd-wants-to-see-more-enforcement.htm](http://www.oecd.org/corruption/australia-takes-major-steps-to-combat-foreign-bribery-but-oecd-wants-to-see-more-enforcement.htm).

²⁹ See *R v. Jousif; R v. I Elomar, R v. M Elomar* [2017] NSWSC 1299, *supra* note 26.

- notify individuals of the purpose for which personal data will be Processed;
- restrict Processing to the purpose for which personal data was collected, except in specific circumstances;
- store personal data securely;
- allow individuals to access their personal data; and
- notify regulators and individuals in the event of certain data breaches.

In addition, the GDPR provides:

- express rights for individuals to require erasure of their personal data (including where no longer necessary for the purpose for which it was collected), to restrict the purpose for which personal data can be Processed, and to withdraw consent for the Processing of personal data;
- scrutiny on consent as a basis for Processing, with implied consent unlikely to be sufficient in most circumstance. Article 7 requires that consent be freely given and that any written consents clearly (and

separately to other issues) specify the purpose for which consent is sought in an intelligible and easily accessible form, using clear and plain language; and

- reporting of any personal data breach, unless it is unlikely to result in a risk to an individual's rights and freedoms. The GDPR also requires organizations to report breaches to the relevant individuals if there is a high risk to their rights and freedoms.

Controllers must also carry out data protection impact assessments and designate data protection officers.

A. Direct Enforcement and Administrative Fines

Under Article 79 of the GDPR, regardless of any action taken by a national supervisory body, each data subject has the right to access judicial processes and seek an effective remedy where they consider their rights have been infringed as a result of non-compliance in Processing personal data. Proceedings may be brought in the courts of the EU member where the Controller or Processor has an establishment, or (except in the case of a public authority

exercising public powers) where the data subject resides.

A person suffering damage as a result of an infringement is also entitled under the GDPR to claim compensation from the Controller or Processor for damage suffered. The Processor is liable to an individual where it has not complied with its obligations or has acted outside or contrary to lawful instructions of the Controller and the Controller is jointly liable unless it proves it was not responsible (likely to be a high bar).

In addition to direct enforcement, national supervisory bodies in the EU will be able to investigate conduct and enforce the GDPR, including by imposing administrative fines for some breaches of up to 20 million EUR or 4% of total worldwide annual turnover in the preceding financial year. The level of fines is determined by national bodies, but are required to be effective, proportionate and dissuasive. The process for deciding to impose a fine is based on the circumstances of the breach and considers not only the nature of the infringement and seriousness, but also the action that led to it, the history of the party, and degree of cooperation with the national body.

B. Extra-Territorial Application

Under Article 3(2), the GDPR will apply to organizations without an EU establishment if Processing of personal data is related to either:

- offering goods or services to data subjects in the EU; or
- monitoring data subjects' behavior as far as it takes place in the EU.

More controversially, under Article 3(1) the GDPR also has application beyond where the Controller has an EU establishment. Article 3(1) extends to situations where Processing "relates" to the activities of an EU establishment, of either the Controller or a Processor. This is very broad and may capture the activities of a non-EU based organization where a subcontractor has an EU establishment that either Processes or is responsible for the Processing of personal data on the organization's behalf. There is no requirement that data subjects be EU residents under Article 3(1).

In this context, even where an organization does not have a presence in the EU, if they use a service provider that Processes their data in connection with the operation of an EU data center, potentially both the non-EU Controller and the EU Processor will be jointly liable under Article 3(1) of the GDPR in respect of the Processing activities. It will be

important for non-EU organizations to have an awareness of who is providing them with services (including any subcontractors) and where they are Processing personal data.

III. Potential Parallels?

Given the description provided above, it will be interesting to see what parallels appear in the development, implementation and enforcement of the GDPR compared with the development, implementation and enforcement of anti-bribery legislation.

Here are some early thoughts:

- **Greater Harmonization:** because the GDPR will apply without the need for national legislation, there is a greater prospect of harmonization in application across jurisdictions. Contrast this with anti-bribery legislation, where inconsistent legislation means that a defense, like facilitation payments, available in some jurisdictions applying the OECD convention is not available in others.
- **Potential Significant Financial Impact:** large financial penalties are a hallmark of FCPA prosecutions in the U.S. The availability of administrative fines of the greater of 20 million EUR or up to 4 % of total worldwide annual turnover in the preceding financial year could see a similar pattern emerge in the enforcement of the GDPR.
- **Approach to Jurisdiction:** regulators and enforcement agencies have traditionally taken an expansive view on jurisdiction in FCPA-style matters. The provisions of the GDPR, and in particular Articles 3(1) and 3(2) suggest that a similar approach will be taken in the enforcement of the GDPR. It will be interesting to see whether a different pattern emerges between attempts at direct enforcement and circumstances in which a supervisory body seeks to levy an administrative fine.
- **Importance of Due Diligence:** knowing who you are doing business

with, or who is doing business on your behalf, is a central part of managing risk in both areas.

- **Rising Tide of Regulation:** the GDPR will impose a higher standard for the protection of the privacy of individuals than under Australian law. Australia has mirrored advances in the anti-bribery space (for example, the introduction of the "failure to prevent bribery" offense in the UK). To the extent that the GDPR represents a higher watermark than current U.S. or Australian data protection regulation, the GDPR could present a sign of things to come in Australia and the U.S.

Perhaps the biggest unknown at this juncture is the enforcement appetite that the regulatory body in each EU state will bring to the task. Administrative fines will be imposed by local regulatory bodies who must ensure that they are effective, proportionate and dissuasive. It will be interesting to see whether there is a level playing field when it comes to enforcement appetite, and the willingness to levy a fine at or close to those available

under the GDPR. As the experience with anti-bribery legislation has shown, similar legislation can see starkly different enforcement outcomes across jurisdictions.

IV. Conclusion

The rising tide of regulation in both the anti-bribery and corruption and personal data space demonstrate that lawyers must keep apprised of international regulatory developments, understand and embrace the complexity of a global rather than local view, and be ready to act decisively to investigate and address any allegations of such conduct.