# EY Asia-Pacific Digital Law Newsletter

## August 2018 - Edition 2

Building a better working world

# Foreword

Welcome to the second issue of the EY Asia Pacific Digital Law Newsletter. We were overwhelmed with your responses to our first issue in January this year and, based on those responses, have decided to:

- Publish the newsletter twice annually, January and August, and keep the quality and quantity of our content similar to the first edition
- Dedicate this second issue to all things cryptocurrency or tokens and Initial Coin Offerings (ICOs)

We have a good range of interesting articles on cryptocurrencies and ICOs, as well as related topics across a number of jurisdictions which we trust you will find of interest. We suspect you will, given the number of requests for us to focus on these areas.

Also, in the "Legal updates" section we provide smaller updates on "Blockchain" and other Digital Law developments occurring across EY regions.

We trust you enjoy the second and special Blockchain edition of the newsletter.

The third issue will be published in January 2019, so please let us know what topics or themes you would like us to address in respect of our articles, either region wide or specific to a particular country.

As noted in our first issue, this is very much your newsletter. So please provide feedback to me (alec.christie@au.ey.com) or our editor Galaad Delval (galaad.delval@cn.ey.com) as to what you would like to see in the newsletter (and thanks to all of you who responded to our first edition).

Just to remind you, "Digital Law" at EY covers everything that may be a legal or regulatory issue or service that is related to digital transformation, e-commerce, e-marketing, information (including privacy and data protection, cyber security and data analytics), intellectual property, IT, Blockchain, smart contracts, artificial intelligence (AI), robotic process automation (RPA),internet of things (IoT), augmented reality (AR), virtual reality (VR), 3D Printing, outsourcing, off-shoring and commercialisation.

We look forward to hearing from you.

Best regards, Alec

Alec Christie
EY Asia-Pacific
Digital Law Leader

# Table of contents

## Articles



## Legal updates





# Crypto clampdown: Australian AML/CTF regime extended to digital currencies

Today, cryptocurrencies are gaining broader appeal and acceptance as people become more comfortable with the underlying technology, while seeing its potential to improve the speed and lower the cost of transactions. Getting the balance right on the regulation of cryptocurrencies has become critical to establishing Australia's position in the international innovation marketplace while protecting the public from malicious use. In a major step to regulate cryptocurrency markets in Australia, the *Anti-Money Laundering and Counter-Terrorism Financing Amendment Act 2017* (Cth) (**AML/CTF Amendment Act**) not only strengthens national security but underpins the building of greater public trust in blockchain and cryptocurrencies, drawing them further into the mainstream.

## What is digital currency?

Cryptocurrencies are an emerging asset class designed to work as a medium of exchange, using cryptographic processes that only a computer can perform as a built-in means of securing value and transfer of ownership. The key feature of cryptocurrencies is that, rather than user trust being founded on the capable management of the currency system by a central bank or similar central authority, trust is engineered into the currency system itself using cryptography.

The *Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth)* (**AML/CTF Act**) has applied to e-currencies for some years, defined as "Internet-based, electronic means of exchange … backed either by precious metal; or bullion…", though it did not cover cryptocurrencies.

Because cryptocurrencies are relying on cryptographic technology to provide assurance as to their value and ownership, they are not encompassed by this definition. The AML/CTF Amendment Act defines a digital currency more broadly, so as to include cryptocurrencies such as Bitcoin and Ethereum.

Under the amended AML/CTF Act digital currency means a digital representation of value that:

- Functions as a medium of exchange, a store of economic value, or as a unit of account
- Is not issued by or under the authority of a government body
- Is interchangeable with money (including through the crediting of an account) and may be used as consideration for the supply of goods or services
- Is generally available to members of the public without any restriction on its use as consideration.

## What is the concern?

Following the 11 September 2001 attacks and revelations in the fallout that shady transactions were funding terrorist activity, the Patriot Act was introduced in the US and similar legislation around the world followed. In Australia, the Australian Transaction Reports and Analysis Centre (AUSTRAC) was granted new responsibilities and powers under the AML/CTF Act to monitor and detect not only money laundering but the financing of terrorist organizations. Under the regime, cash transactions of A$10,000 or more as well as suspicious transactions and international transfers occur under the watchful eye of AUSTRAC's monitoring and enforcement teams.

Today, money laundering remains a key enabler of criminal activity including drug trafficking, tax evasion, people smuggling, fraud and corruption imperiling human lives and livelihoods and at great cost to the economy. In Australia alone, the economic cost is estimated to be in the tens of billions of Australian dollars. AML/CTF laws need to keep pace with trends and developments, including those in technology, so as to minimize scope for criminals to circumvent controls and avoid detection.

As digital currencies, including cryptocurrencies, have been allowed to exist largely outside the regulated financial system, while growing in market size and adoption, they have given rise to new risks and opened new means by which criminal activity can be facilitated undetected. From its earliest days, Bitcoin became the currency of choice for black market transactions carried out on the dark web.

The money-laundering and terrorism-financing problem is generally

addressed through "Know Your Customer" (KYC) obligations. Until now, these requirements have not been enforced on cryptocurrency exchanges.

## What has changed?

The AML/CTF Amendment Act has made three key sets of changes:

- It provides some relief by easing the weight of regulation on low-risk activities.
- It grants new powers and functions to the AUSTRAC's CEO.
- It subjects digital currency exchange providers to the existing AML/CTF regime.

The amendments noted in the third key change are of most relevance. The existing AML/CTF obligations now extend to digital currency exchange providers where they previously did not. Under the amended AML/CTF Act, digital currency exchange providers' obligations include:

- Enrolling and registering their details on the Digital Currency Exchange Register maintained by AUSTRAC. Penalties for a breach are imprisonment for two years and a potential penalty of A$105,000.
- Establishing and maintaining an AML/CTF program to identify, mitigate and manage money laundering and terrorism financing risks.
- Identifying and properly verifying customer identities. This is a positive obligation to put in place effective KYC processes that appropriately verify the human owners of accounts opened on the exchange.
- Reporting to AUSTRAC suspicious activities and transactions involving fiat amounts of A$10,000 or more. This empowers AUSTRAC with more intelligence to effectively monitor activity including cryptocurrency trades.
- Maintaining records relating to transactions including customer identification for seven years.

## Knowing cryptocurrencies' "customers"

These reforms compel digital currency exchanges to implement and maintain an AML/CTF program. Typically, this involves:

- Conducting risk assessments
- Including understanding users of the cryptocurrency exchange, the means by which the services are provided and the jurisdictions across which exchange is conducted
- Regular independent review of the program
- An employee screening program
- Carrying out risk awareness training for employees
- Various customer due diligence protocols including trust verification procedures, identifying and verifying beneficial owners and handling discrepancies discovered in identity information
- Transaction monitoring
- Reporting to AUSTRAC

Under the AML/CTF Amendment Act, the AUSTRAC CEO gains the power to:

- Issue infringement notices for a greater number of offenses including non-compliance with KYC, reporting and record-keeping obligations. Prior to these changes, for most offenses a penalty would only be imposed following enforcement proceedings in the Federal Court of Australia. With the new powers, AUSTRAC can more effectively police the regime.
- Issue remedial directions requiring a reporting entity under the AML/CTF Act to comply with a breached obligation. If, for example, a reporting entity failed to comply with its reporting obligations under the AML/CTF Act, even up to two years in the past, the AUSTRAC CEO can compel the reporting entity into remedial action.

For many who might wish to use cryptocurrency exchanges for illicit purposes, the risks of being caught using an exchange to facilitate their activities will become too great and they will choose not to. The impact on cryptocurrency ecosystems is therefore a "clean-up" – the purging of unwanted operators and transactions from the ecosystem.

These measures are not bullet-proof. Those who rely on laundering processes will continue to find ways to do it, albeit with greater effort and higher cost. What these measures achieve, though, is to put AUSTRAC in a better position to monitor and crack down on illicit activities and more easily stay abreast of how cryptocurrencies are being used.

## Looking ahead

These changes are only part of a series of regulatory updates recognizing both the opportunities and risks associated with cryptocurrencies and related payments technologies. Since 2017, digital currencies have no longer been subject to double taxation in Australia, which had been driving investment in cryptocurrency technology overseas.

It remains to be seen how other government and quasi-government agencies around Australia will respond to the uptake of digital currencies in Australia. We expect to see more reports and investigations and further reforms to the overall regulatory framework, particularly relating to the protection of consumers and investors.

**Authors**

Alec Christie, Partner, EY Asia-Pacific Digital Law Leader, Ernst & Young (Australia)

James Wong, Solicitor, Digital Law, Ernst & Young (Australia)

# Understanding the status of cryptocurrencies in Mainland China

The development of cryptocurrencies in Mainland China has had an interesting impact on the value and development of cryptocurrencies worldwide. For example, in late 2013 when the People's Bank of China, Ministry of Industry and Information Technology, China Banking Regulatory Commission, China Securities Regulatory Commission and China Insurance Regulatory Commission jointly issued the Circular on the Prevention of Risks from Bitcoin, Bitcoin lost almost half of its value before bouncing back and then fluctuating for a few days.

Since then there has been a worldwide interest on the regulatory actions occurring in Mainland China, as well as how is the Chinese government reacting to and willing to further develop cryptocurrencies and blockchain technology. This information has been driving some of the fluctuation of the global cryptocurrency markets as well as the adoption and growth of blockchain technology in Mainland China, depending on how welcoming the Mainland China market was.

While in recent years the future of Bitcoin and other cryptocurrencies seemed to stabilize, albeit remaining tumultuous in Mainland China, they remained under scrutiny by multiple regulatory bodies to prevent abuses. This status quo ended through an increased concern over Initial Coin Offerings (ICOs) being used for fraud and scam purposes in Mainland China. As a result the National Internet Finance Association of China (NIFA) issued an important warning on 30 August 2017 on the risks linked to ICOs, the first step toward a crackdown on cryptocurrencies' ecosystems.

## Banning ICOs and exchanges from Mainland China

On 4 September 2017 cryptocurrencies encountered a major setback in Mainland China with the publication of the Announcement on preventing ICOs risks (关于防范代币发行融资风险的公告). Issued simultaneously by seven governmental bodies, the Announcement included in Article 2 that "all kinds of ICO activities shall be discontinued immediately from the date when this Announcement is issued." However, the Announcement's target was broader, with Article 3 aimed at clamping down on cryptocurrencies exchanges stating that "any of so-called token financing and trading platforms may not engage in the exchange services between any legal tender and tokens or between cryptocurrencies, or engage in the sale of tokens or cryptocurrencies."

The Announcement has had immediate effects, with major trading platforms stopping their cryptocurrency exchanges in Mainland China. Some of them were also reported to have moved their operations from Mainland China to overseas, such as to Hong Kong or Singapore. However, local users were still able to participate in ICOs and exchanges of cryptocurrencies through overseas platforms, despite the ban. An announcement from the NIFA on 26 January 2018 made public this issue. It was then followed by a public government announcement that regulatory measures would be taken against overseas websites providing cryptocurrency trading services to Mainland China. It is noticeable that, currently, no national regulatory actions have been taken against foreign exchange platforms with most of them still accessible from Mainland China.

## The orderly exit of Bitcoin mining

A few months following the initial ban on ICOs in Mainland China, a request was made by the Leading Group of Internet Financial Risks Remediation to local government to promote an orderly exit of Bitcoin mining for companies engaging in such businesses. As a result, tighter local Bitcoin mining regulations have been observed, which are deemed to have led to the shutdown of some Bitcoin mining operations, however, major Bitcoin mining companies have kept a presence in Mainland China while publicly discussing their migration toward jurisdictions favorable to their activities. Smaller operations have continued their mining activities in Mainland China.

It is difficult to assess whether the orderly exit from Bitcoin mining has been a success or not due to the remaining amount of Bitcoin mining

companies and their operations in Mainland China. However, it is impossible to deny that the latest regulatory moves have impacted the cryptocurrency markets in Mainland China. The People's Bank of China (PBoC) reported that its measures against ICOs and trading platforms have been successful in diminishing the part played by the Chinese Renminbi in the global Bitcoin transactions share to under 1 percent. It has also been reported that, since September 2017, 88 cryptocurrency trading platforms and 85 ICO exchanges have been shut-down, although no mention was made of mining operations.

## Toward a national cryptocurrency

Despite this visible crackdown on cryptocurrencies in Mainland China, it is important to note that the ultimate target was to further regulate cryptocurrencies and not to strictly ban or prevent Blockchain technologies to emerge. This is further supported by regular announcements and projects from the PBoC on the development of its own national cryptocurrency.

The interest of the PBoC to create a national cryptocurrency can be tracked as far back as 2014 with the creation of a dedicated research team, as explained in a statement issued by the PBoC on 20 January 2016. Since then it was reported that the PBoC was conducting research and trial runs, with the conclusion of their trials for the algorithms supporting the future cryptocurrency reached by October 2017.

More precision was given on 9 March 2018 by the governor of the PBoC during a conference, where it was confirmed that the PBoC was still actively working on the development on a national cryptocurrency while affirming that the project was not to be rushed to prevent any negative consequences.

## A strong interest toward blockchain technology

It must be noted that the Chinese authorities are still showing a strong interest in the development of Blockchain. Whether it be from President Xi Jinping in his speech made on 25 May 2018 or from the 9 August 2018 statement of the Ministry of Industry and Information Technology, the general trend is toward contemplating means to accelerate the promotion of Blockchain-based technologies and applications in Mainland China. This interest can be seen in the market with the increase of companies leveraging Blockchain technologies in the provision of services and in the increase of governmental projects also leveraging Blockchain technologies.

Despite ICOs being banned and mining operations for major cryptocurrencies in Mainland China, reducing such developments should not be understood as the end of cryptocurrencies and Blockchain technology in Mainland China. Again, the ban on ICOs is not a ban on the use of cryptocurrencies or any Blockchain leveraging tokenization. Furthermore the PBoC is pushing toward trials for its future national cryptocurrency, in addition to the desire by the government to see blockchain technologies further researched and implemented show that Mainland China still welcomes Blockchain related innovations. To sum up, we believe that companies willing to develop blockchain related services are welcomed in Mainland China, although companies solely planning to offer cryptocurrency related services and products will currently find it difficult (or impossible) to integrate into the Chinese market.

**Authors**

Dr. Zhong Lin, Managing Partner, EY Law Firm

Galaad Delval, Data Protection Officer, EY Law Firm

# The evolution of Initial Coin Offering regulation in New Zealand

An evolving understanding and approach to the regulation of ICOs in New Zealand seeks to encourage innovation while still protecting investors.

ICOs aligned to the issue of traditional securities will be covered in New Zealand by securities regulations. But as more utility tokens enter the market, the regulator appears to be aiming to encourage innovation while still ensuring investors are appropriately protected.

## What is an ICO?

Initial Coin Offerings (ICOs) enable the raising of funds from investors through the issue of cryptocurrency tokens. The digital tokens that investors receive carry certain rights, such as access to a new product or service, or an interest in an underlying asset or project.

## Are ICOs regulated as securities in New Zealand?

Yes, if they are come within the definition of financial product under the Financial Markets Conduct Act 2013 (FMCA) and are offered to retail investors in New Zealand. The Financial Markets Authority (FMA) clarified this position in late 2017. A token's specific characteristics and economic substance will determine whether a token is a financial product. As well as the four types of financial products defined in the FMCA (debt securities, equity securities, managed investment products and derivatives), the FMA also has broad powers to designate a token as a financial product if it considers that necessary for reasons such as the promotion of fair and efficient financial markets in New Zealand.

For the FMCA to apply, it must also be offered to retail investors in New Zealand. If it is, and it can be classed as a financial product, then issuers will have various disclosure, governance, licensing and financial reporting obligations under the FMCA, as well as anti-money laundering and general consumer protection obligations.

## How are New Zealand start-ups responding to regulation?

As the FMCA obligations can be onerous, time consuming and expensive to comply with, many token issuers (often start ups) are structuring their ICOs so the FMCA does not apply.

A recent high profile example is Centrality, an Auckland-based Blockchain-enabled marketplace. Centrality raised US$80m in just six minutes when it issued its CENNZ token via a Token Generating Event (TGE) - making it one of the most successful ICOs to date. This came on top of the US$15m in Ethereum that Centrality had raised previously from a pre-sale. The CENNZ is a utility token that can be used on Centrality's platform to buy software and other blockchain-enabled services and applications.

The CENNZ white paper makes for interesting reading in the context of the FMCA. It purports to exclude various potential categories of investor via statements that the TGE is not "to be construed as an offer of financial products to any person who requires disclosure" under the FMCA. It goes on to provide that the CENNZ tokens are not being "offered for sale in New Zealand to any person who requires disclosure" under the FMCA in relation to regulated offers.

The white paper also emphasizes that the TGE is not a retail securities offer and is "under no circumstances to be construed as an offer to sell or issue, or a solicitation of an offer to purchase or subscribe for, any securities to any retail investor in any jurisdiction". Applicants for the purchase of CENNZ tokens are required to "irrevocably and unconditionally" represent and agree to various wholesale investor warranties and selling restrictions including that they are not citizens or residents of China, the USA or any other country where the trading of tokens issued pursuant to a TGE is not permitted by law.

## Expected clarifications from the FMA

The upshot of all this from a New Zealand law perspective is that the FMCA does not apply. The FMA has yet to publicly comment on the Centrality TGE or the approach adopted around the issue of the CENNZ token. However we understand that further FMA guidance clarifying the regulatory position of cryptocurrencies in New Zealand is expected shortly – and it is likely to confirm that tokens

issued to wholesale investors or investors outside New Zealand only will not be subject to the full licensing, governance and disclosure requirements of the FMCA. They will, however, still have to comply with the FMCA's fair dealing consumer protection requirements, which prohibit misleading or deceptive conduct and false, misleading or unsubstantiated representations.

The FMA is also expected to clarify that utility tokens like CENNZ will not be considered financial products. They may, however, constitute a financial service requiring compliance with the Financial Service Providers (Registration and Dispute Resolution) Act 2008. Financial services include:

- Issuing and managing a means of payment, such as an exchange issuing its own cryptocurrency to facilitate trading.
- Operating a value transfer service, such as an exchange or wallet provider allowing cryptocurrency trading.

To navigate the various regulatory requirements, ICO white papers will need to be carefully written to provide investors with appropriate, transparent information about the nature of the token, who may invest and what rights they will receive, as well as meeting fair dealing requirements and complying with anti-money laundering and general consumer protection law requirements.

## Investor protections

The FMA has demonstrated before that it takes investor protection issues seriously. In November 2017 it raised concerns over the accuracy of statements made in offer documents by an Auckland university student planning to raise NZ$220m through an ICO for an e-commerce site. The FMA stated that it "expects investors to be provided with accurate and understandable information to assist then to make decisions relating to financial products ... When the FMA sees this has not happened we will take action to protect investors." The student canceled the ICO a week after the FMA warning.

## Conclusion

The FMA is keen to be seen as supportive of innovation in the New Zealand financial services industry, particularly given that one of the purposes of the FMCA is "to promote innovation and flexibility in financial markets". However, the FMA must balance those goals against its responsibility to protect investors, ensuring risks are not passed on to investors in ways they don't understand.

Accordingly, anyone seeking to raise funds in New Zealand using an ICO, or to set up any form of cryptocurrency exchange or market, should ensure their communications with potential investors reflect their various obligations, including in relation to the fair dealing consumer protection requirements. It's also worth engaging with the FMA early to take them on the journey with you.

**Author**

Frith Tweedie, Senior Manager, EY Law Limited

# Australia

The consultation/exposure draft of the Treasury Laws Amendment (Consumer Data Right) Bill 2018 (CDR Bill) has just been released. The CDR Bill introduces the much discussed and somewhat controversial Consumer Data Right (CDR) recommended earlier in the year by the Productivity Commission.

While the stated focus of the CDR Bill is to introduce the CDR into the Banking, Energy and Telecommunications sectors, it may be extended to other sectors by regulation. "Open Banking" is to be the "first cab of the rank" and is to be effective by 1 July 2019.

CDR data is information that is to be separately specified/designated for each sector but includes information which is derived (wholly or partly) from that data. While yet to be designated in the "Open Banking" context it has been flagged as all information provided by a consumer to a bank and their transaction data. However, given the definition includes all information "derived from" that information then all analysis and value added uses of all consumer provided and transaction information will be CDR data and subject to the CDR rights and obligations, including the right for consumers to transport such value added information to a third party competitors.

At its heart, the CDR Bill builds on the rights of individuals under existing Australian privacy law to access CDR data about themselves from organizations that hold it by:

- Adding additional rights for individuals and obligations for organizations
- Extending these additional rights to small businesses and non-personal information
- Extending the new obligations to organizations/ those not currently subject to the Privacy Act
- Significantly increasing the potential fines, when such fines can be levied and introducing imprisonment for up to 5 years for certain CDR data related crimes,

in order to clearly establish that the CDR data belongs to the consumer and to allow the "free movement" of that data, at the direction of the consumer, among and between businesses within the sector. It is hoped this will level the playing field between the big/established (data rich) businesses and the new/start up (data poor) businesses in that sector, easing the way for new entrants.

In addition to increased funding for the regulators, the main additional and new rights and obligations in respect of CDR data for those sectors in which it is introduced are:

- Increased (or "genuine") express consent requirements for disclosure and use of one's CDR data
- The right to withdraw consent to disclosure and use of one's CDR data
- An additional regulator (the ACCC) to have oversight of the CDR while the Privacy Commissioner continues to oversee privacy law compliance in respect of the CDR data
- All recipients of CDR data to be subject to Australian privacy law (even those who would ordinarily not be covered by such)
- It will apply to legal persons (not just individuals). That is, small company data is covered and the CDR rights are also exercisable by small companies
- It will have a larger/broader extraterritorial footprint. That is, entities not "carrying on

business" in Australia may be caught by the CDR

- A direct right of action (including class actions) for consumers to seek compensation for breaches of the CDR
- Transportability of one's CDR data
- Only "certified" data recipients may receive, use and have disclosed to them CDR data
- "Equivalent but more onerous" versions of the existing privacy obligations (under the APPs) will apply to CDR data
- Fines of up to the greater of 10% of annual turnover and $10m may be imposed for certain CDR breaches and imprisonment for up to 5 years, on conviction, may be imposed for misleading consumers in respect of use of the CDR system and/or their accreditation

There is a fear that the CDR Bill will create a two (possibly more) class privacy regime where the level of protections and rights one has depends on whether one's data falls within CDR for a regulated sector or is simply personal information in a non regulated sector.

In addition, regulations and rules which are to be promulgated by the regulator (the ACCC) may seek to apply different "rules" in relation to the CDR within a regulated sector. This will cause yet further stratification of rights and obligations, not only between regulated or non regulated sectors but also within regulated sectors, causing confusion about what rights and obligations apply, when and to whom (noting that the character of specific data, and thus the rights and obligations applying to it, may change and change back several times over its lifetime). Of course, this confusion is likely to translate into significant additional costs for businesses and thus, ultimately, consumers.

# Hong Kong

There has been a surge in Blockchain-based companies raising capital by way of Initial Coin Offerings (ICOs). The Hong Kong regulators (the Securities and Futures Commission (SFC)) have responded by seeking to regulate the selling, purchasing, brokering and advertising of digital coins to ICO investors. Such investors and ICOs are typically willing to buy digital coins for a share in the Blockchain-based companies' investments.

In February 2018, the SFC issued reminders to multiple cryptocurrency exchanges in Hong Kong warning them that cryptocurrencies may constitute securities under the Securities and Futures Ordinance (SFO) and thus may require licensing, in particular, when dealing with ICOs. In light of this, the SFC took action against an ICO issuer (Black Cell Technology Limited) in March 2018 which sold digital coins to investors (which could be redeemed for equity shares in the company) for proceeds to be used to fund the development of a mobile application.

Under such an ICO arrangement, the SFC considered this was a collective investment scheme (CIS) and thus was regarded as securities under the SFO, which resulted in the company halting its ICO and undertaking not to set up any scheme that constitutes a CIS, unless it complied with the regulatory requirements.

# Japan

More than one year has passed since the regulation on Virtual Currency Exchange Service Providers (VCESP) was adopted and enforced as of April 2017.

Ever since, business operators are required to be registered when they are considered to be VCESP when engaging in either:

- Selling or purchasing virtual currency, as well as providing exchange services toward another virtual currency
- Serving as intermediary, agency or delegation for the sell, purchase or exchange of virtual currency
- Managing users' money or virtual currency in connection with the sell, purchase or exchange or virtual currency

In order to be registered, business operators need to satisfy certain requirements (including duty of separate management of customers' assets and its own assets, and setting up system with sufficient information security) set under the Payment Services Act of Japan.

In January 2018, approximately JPY58b of virtual currency "NEM" was lost from one of the largest VCESPs in Japan (it is suspected to be the action of crackers), and as a result the Financial Services Agency (FSA) of Japan began to strengthen the enforcement of the regulations, while launching audits at VCESPs. Since then, the FSA issued warnings to two foreign virtual currency operators who solicited Japanese customers without registration, and issued business suspension order to six VCESPs.

# Mainland China

Following the enforcement of the Cybersecurity Law in 2017, data protection has been supplemented with a new standard for personal information, the GB/T 35273-2017, also called Information Security Technology - Personal information security specification (the Specification) published in December 2017 and enforced as of 1 May 2018.

The Specification is the latest recommended standard by the National Information Security Standardization Technical Committee regarding the definition of personal information and their use within Mainland China. The direct successor to the GB/Z 28828-2012 standard, a National Guiding Technical Document titled the Information Security Information Guidance on Protection of Personal Information of Public and Commercial Service Information System, it further details best practices on the collection, use, transfer and deletion of personal information in Mainland China.

Among the most important points covered by the Specification can be found a with detailed and expanded definition of sensitive personal information. The list can be quite surprising for companies located in the EU as the definition also includes personal information, such as phone numbers and identification document information. However, it is important to note that such personal information is linked to other regulations within the Chinese legal ecosystem that gives them a critical weight in one's personal life. Beyond the definition of sensitive personal information, the Specification also further refined the definition of what is consent within Mainland China, as well as what is an informed consent. The Specification also supports network operators by providing a clear guidance on how such consent should be proceeded, namely through the inclusion of an appendix on how a privacy notice can be formulated to be compliant.

While the Specification is not a binding text, companies should be made aware that the interpretation on data protection in Mainland China made by the Specification is a major step forward. Therefore, it is advisable, when planning compliance of data protection and cybersecurity in Mainland China, to keep the Specification in mind.

# New Zealand

New Zealand recently introduced a new Privacy Bill to update its 25 year old privacy legislation. But does the Bill go far enough to encourage organizations to take privacy seriously? Or is it out of step with global privacy law reforms, increasing the risk of New Zealand losing its coveted EU adequacy status?

New Zealand's Privacy Act 1993 has just had its 25th birthday. Over that time, the way businesses collect, store and use data has undergone significant change. The explosion of data-driven technologies and a growing range of threats to individuals' privacy rights makes privacy regulation of ever-increasing importance.

The recently introduced Privacy Bill aims to address those issues and keep up with global privacy law reform. However, while the new Bill introduces some key changes to current requirements, overall there are questions as to whether the current draft goes far enough.

## Mandatory data breach notifications

The Privacy Bill introduces mandatory reporting of data breaches to New Zealand. Unless exceptions apply, privacy breaches that pose a risk of harm to people must be notified to the Privacy Commissioner and affected individuals as soon as practicable after the agency becomes aware of the breach. The "as soon as practicable" time frame is used in Australia's equivalent legislation and appears to be less onerous than the 72-hour window prescribed by Europe's General Data Protection Regulation (GDPR).

Failure to notify in the prescribed way is an offence that could result in a maximum fine of NZ$10,000.

## New powers for Privacy Commissioner

The Privacy Commissioner receives new powers to issue compliance notices requiring an agency to do something - or stop doing something - to comply with privacy law. The Commissioner will also have stronger investigation powers that permit the shortening of time frames for compliance and allow stronger penalties for non-compliance. She will also be able to make binding decisions on complaints relating to access requests, rather than the Human Rights Review Tribunal (which will be the appeal body).

## Cross-border protections

The Bill requires New Zealand organizations disclosing personal information overseas (including for offshore cloud storage) to take reasonable steps to ensure such personal information is subject to acceptable privacy standards. Overseas disclosure is prohibited unless the individual(s) concerned have consented, the overseas country has been specified in regulation as have comparable privacy laws to those of New Zealand, or where there are reasonable grounds to believe the overseas person is required to protect the information using comparable safeguards to those in the Bill – for example via contract.

## New criminal offenses

New criminal offenses are introduced for misleading agencies in ways that affect other individuals' personal information, making false or misleading statements to the Office of the Privacy Commission, making false representations of authority under privacy laws and knowingly destroying documents containing personal information following receipt of an access request.

Any person committing one of those offenses will be liable to a fine of up to NZ$10,000.

## Recommendations not taken up

Despite those changes, the current draft of the Privacy Bill does not include many of the recommendations previously made by the Privacy Commissioner. As he puts it, the Bill is fit for purpose for 2011, which is when the New Zealand Law Commission recommended privacy law reform. Seven years is a long time given the current rate of digital change.

The Bill is also out of step with a number of key changes introduced by the GDPR. The Bill does not include rules around data portability (also recommended by the Privacy Commissioner) or the right to be forgotten. Also absent are requirements for unambiguous consent, Privacy by Design and Privacy Impact Assessments, demonstrable accountability and increased protection for minors.

Most noticeably, the Bill fails to introduce the fines recommended by the Commissioner: NZ$1m for corporates and NZ$100,000 for individuals. Instead, the new maximum fine is NZ$10,000, which is significantly lower than the Privacy Commissioner's recommendations and equivalent maximum fines under the GPDR and in Australia.

Arguably the new fines do not provide sufficient incentive for organizations to make any significant improvements to their privacy-related activities. As the Privacy Commissioner has stated, without real and meaningful consequences for non-compliance, rogue agencies will continue to thumb their nose at the regulation, meaning responsible organizations will disproportionately bear the cost of compliance, while delinquent corporations will ignore their obligations.

An unscrupulous business could choose to risk a NZ$10,000 fine rather than face the reputational risks associated with public notification of a data breach.

## Adequacy

New Zealand also risks losing its coveted adequacy status if its once world-leading privacy laws slip behind international developments. The European Commission formally ruled in December 2012 that New Zealand's privacy law provided an 'adequate level' of privacy protection to meet European standards. That means personal information can legally be sent to New Zealand from Europe for processing without special additional measures being taken by European companies. Given the lack of various GDPR rights and equivalent accountability requirements in New Zealand law, there is a risk the European Commission will conclude that New Zealand privacy laws no longer meet revised EU standards under the GDPR.

The Bill is currently at the select committee stage after passing its first reading, with public submissions now closed. The questions now will be whether the submissions are addressed in any revisions to the draft Bill.

# Vietnam

Following the Law on Cyber Information Security No. 86/2015/QH13 of 19 November 2015, Vietnam's main legislative body, the National Assembly on 12 June 2018 passed a new Law on Cyber Security (LOCS). It is designed for the protection of national security, combating cybercrime and promotion of digital safety on the internet.

The LOCS prohibits the use of the cyberspace to perform certain acts including:

- To organize, carry out, collude, urge, bribe, dupe, entice, train, or coach people to oppose the State of the Socialist Republic of Vietnam.
- Distort historical truths, denying revolutionary achievements, destroying the great unity of the people of all ethnic groups, offending religions, practicing racial and sex discrimination.
- Posting false information intended to make people afraid, cause damage to the socio-economic environment.
- To incite, embroil or arouse other person to commit with a crime.

Additionally, the LOCS requires all foreign providers of internet related services to open representative offices and data localization centers in Vietnam, where the information of Vietnam based users must be stored.

The LOCS grants the Ministry of Public Security the power to demand access to any organization's or company's data systems for investigation in cases where there is a perceived threat to national security and against this law.

The new law will come into effect on the 1 January 2019 and we await further guidance on its implementation.


June
S M T W T F S
1 2 3 4 5 6 7
8 9 10 11 12 13 14
15 16 17 18 19 20 21
22 23 24 25 26 27 28
29 30

# Contacts

## EY Asia-Pacific Digital Law services contacts


**Australia**
Alec Christie
alec.christie@au.ey.com
+61 2 9248 4325

**Hong Kong**
Harry Lin
harry.lin@laa.hk
+852 2629 3201

**Japan**
Kotaro Okamoto
kotaro.okamoto@jp.ey.com
+81 3 3509 1669

**Mainland China**
Dr. Zhong Lin
zhong.lin@cn.ey.com
+86 21 2228 8358

**New Zealand**
Frith Tweedie
frith.tweedie@nz.ey.com
+64 27 836 1545

**Singapore**
Evelyn Ang
evelyn.ang@sg.ey.com
+65 6718 1288

**Vietnam**
Thinh Xuan Than
thinh.xuan.than@vn.ey.com
+84 8 3824 5252


**For further inquiries on Digital Law services, please visit our website**
**ey.com/gl/en/services/tax/law/ey-law-digital-law**

**EY** | Assurance | Tax | Transactions | Advisory

About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.


EYG no. 010995-18Gbl
ED None



ey.com/gl/en/services/tax/law/ey-law-digital-law