Asia Pacific Data Protection and Cyber Security Guide 2019
Asia-Pacific Data Protection and Cyber Security Regulation: 2018 in review and looking ahead to 2019

2018 stands as one of the most significant years yet for the development of data protection and cyber security regulation globally, spearheaded by the May, 2018 implementation of the European Union’s General Data Protection Regulation (the “GDPR”) and marked by a number of significant data breaches and enforcement actions.

The Asia-Pacific (“APAC”) region saw significant regulatory developments of its own and was by no means immune to the growing cyber threat. According to figures compiled by digital security provider Gemalto, APAC accounted for thirty-six percent of the global number of reported cyber security events, a proportion that may well increase as mandatory data breach notification laws start to take hold in the region. The call to action on cyber security in APAC has never been more pressing.

One of the most striking regulatory developments in 2018 was India’s decision to chart a course for the introduction of a comprehensive data protection law. The draft bill currently under review draws heavily from innovations reflected in the GDPR, such as extra-territorial reach based on the targeting of business in India and maximum fines tracking four percent of an offender’s worldwide turnover.

China introduced a GDPR-inspired national standard in May, 2018. Although non-binding, the standard has been taken as a key reference point for organizations seeking to comply with the often general and vague data protection requirements of China’s Cyber Security Law and other data protection regulatory requirements. The highly controversial data localization requirement under the Cyber Security Law continues to cast a shadow of uncertainty, with the formal implementing measures for security reviews of international data transfers not yet finalized.

China’s Cyber Security Law

It is now over a year and a half since China implemented its Cyber Security Law, and yet critical areas of the law remain unspecified. Expectations that clarity would emerge through detailed implementing measures having been repeatedly dashed. It is clear enough that the impact on international business has been significant, and this is on-going. The uncertainty surrounding the law has in and of itself been sufficient to force businesses to make decisions now about their data processing and technology infrastructure in China.

We explain the Cyber Security Law in more detail in the China “Spotlight” section below, but to briefly summarize the key impacts:

• **Data Localization:** The law’s data export review procedure has not yet been fully elaborated. What seems clear is that the measure amounts to data localization in relation to personal data and “important data” collected in China by “operators of critical information infrastructure”. The potential extension of the data export review measure to “network operators” would effectively sweep in any and all businesses with operations on the ground in China. Expectations are that these businesses will be subject to a self-assessment of the necessity and security of their data exports, with materiality thresholds triggering...
an obligation to report the export to authorities. Whether or not such a report would lead to a substantive review of international transfers remains to be seen.

- **Exclusion of Foreign Technology:**
The intensive regulation of the information security of operators of critical information infrastructure is broadly in line with international developments in cyber security regulation. However, a key aspect for multi national businesses is the extent to which regulations will (explicitly or by implication) close aspects of the Chinese market to foreign technology and services, at least in respect of key network infrastructure.

The impact of the introduction of the Cyber Security Law has been compounded by a broader tightening of the regulation of China’s internet. China’s censorship of media and communications is of course nothing new. For years many internet users in China relied on virtual private networks (“VPNs”) and other technologies to bypass what has come to be known as the “Great Firewall of China” (the “GFC”) to receive uncensored internet access. VPN services are subject to licensing in China and cannot lawfully deliver unfiltered internet content. China has cracked down on illegal VPN services breaching the GFC in the past, but the pattern of administrative action commencing in 2017 has been far more comprehensive and effective than in the past. The authorities have required telecommunications service providers to more rigorously monitor their networks to identify illegal VPN services and require that their customers obtain proper licensing for onshore hosted content. Administrative practices allowing multi-national corporations to extend their global wide area networks to end users in China generally remain in place, but these arrangements must be examined carefully to understand whether or not they fall within the retrenched administrative tolerances.

China has long been considered inconsistent in its enforcement of its patchwork of laws, measures and standards concerning data protection. Enforcement under the Cyber Security Law appears to mark a stepping up of expectations in relation to private sector handling of personal data. China too has fallen victim to increasing scale of hacking and data breach incidents. For example, reports emerged in August, 2018 that a Chinese hotel group had suffered a breach in relation to 130 million guest records.

**The Impact of the GDPR**
The GDPR, implemented in the EU in May, 2018, has generated shockwaves globally. The immediate impact for businesses headquartered in the APAC region has been the extension of the scope of application of European data protection law from an “establishment” concept limiting the law’s application to organizations with “bricks and mortar” operations on the ground in the EU to a broader set of criteria making the GDPR applicable to APAC businesses offering goods and services online to data subjects in the EU. The prospect of penalties reaching four percent of world-wide turn-over has caught the attention of many APAC-based businesses, and so we see concerted compliance activity with a view to understanding the extent to which the new European requirements apply to businesses headquartered here. In some cases, organizations’ operations can be restructured so as to avoid “over-compliance” with EU requirements. In many cases, however, the international scope of business necessitates a GDPR compliance exercise in respect of at least some of the organization’s operations.

The impact of the GDPR for APAC is much farther reaching than the compliance requirements for regional businesses with EU touchpoints. Lawmakers and data protection authorities across the region are studying the GDPR with a view to reforming their own regimes to reflect this the version 2.0 upgrade of comprehensive data protection regulation.

More important to the evolution of laws in the APAC region, however, is the fact that there is far greater demand for data protection in the region now, as citizens become increasingly immersed in a new digital reality brought about by widespread use of mobile handsets and the emergence of the internet of things. At the same time, governments in the region are moving concertedly towards digital identity programs and more invasive approaches to electronic surveillance. On this view, the apparent “cherry-picking” of GDPR concepts is a reflection of perceived need in the region for laws that are more protective.

To take an example, the recent introduction of mandatory data breach notification laws in Australia and the Philippines has been followed by draft measures in Singapore and India. Hong Kong, Singapore and Japan already have voluntary data breach notification regimes in place. As the headlines fill with accounts of large scale personal
data breaches, the move towards mandatory breach notification seems all but inevitable.

**India’s “Fourth Way”**

The GDPR’s influence is extensively seen in India’s draft Data Protection Bill, tabled by India’s Committee of Experts, under the chairmanship of Justice B.N. Srikrishna alongside a detailed report entitled “A Free and Fair Digital Economy – Protecting Privacy, Empowering Indians”. Whilst we expect to see vigorous and robust debate on the Bill in the coming months, a move by India towards truly comprehensive data protection regulation is a significant step for the APAC region, given that India is likely to be the region’s most populous nation by 2025.

The Srikrishna Committee in the Committee Report promises the approach set out in the Bill to be a “template for the developing world”, a “Fourth Way” that attempts a triangulation amongst the three existing models of data protection regulation put forward by the US, the EU and China respectively. The Srikrishna Committee writes that the “Fourth Way” should reflect India’s unique understanding of the appropriate balance to be struck between individual freedoms recognized by its Supreme Court in the Puttaswamy decision and the common good.

It raises a number of striking points of comparison to international developments. At a high level, many of the Bill’s provisions suggest that the Fourth Way is most closely aligned to positions taken in the GDPR, lending further support to the notion that the GDPR has already fixed some critical sign-posts for the trend of legislative developments in the APAC region. There are, however, important departures here, and much will need to be resolved in the details.

There has been much critical commentary on the Bill in India across a range of issues. Some focus on how government use of personal data would be constrained under the law, a key issue in light of privacy concerns already raised in connection with India’s Aadhaar biometric-based identity system.

The data localization measure has also attracted significant attention, representing a clear outlier from the Bill’s overall alignment with the GDPR. The technology sector in India has raised concerns about this measure, which could hinder the international expansion of Indian technology businesses, and would of course impose constraints on market access to India by foreign-based players. More broadly, there are concerns that ambitions
for a growing and robust technology sector, stated to be a key ambition for India, are not best served by alignment with the EU model.

**Regional harmonisation, adequacy, inter-operability?**

With the data protection compliance burden growing so rapidly in the APAC region, multinational organisations have good reason to hope for some measure of harmonisation of compliance standards, including practical solutions for cross-border data transfers.

The 2004 APEC Privacy Framework provided some rough sign-posts for a common approach to principles-based data protection regulation in the region. But while the common themes of the APEC framework are well-evident in national data protection laws across the region, it is clear that a strict harmonization of laws is unlikely.

We do see effective compliance solutions that, in broad terms, track a “reasonable high water mark” of in-country practices and policies meeting most requirements across the region. This approach, however, necessarily leaves specific points of compliance to be addressed. A salient example is the area of direct marketing, which will have implications under most jurisdictions’ data protection laws, but which may involve technical requirements that are specific to each jurisdiction, whether under the data protection law itself or under anti-spam laws, internet regulation or consumer protection laws. The result on this front is definitely a patchwork, with some jurisdictions requiring discrete or unbundled opt-in or opt-out consents, sometimes with exemptions, sometimes without, some jurisdictions having “do not call” registries and some jurisdictions having specific formalities that must be adhered to in direct marketing communications, such as incorporating “ADV” or some equivalent form of indicator in message headings.

Offshore data collection and cross-border transfers have emerged as a particularly challenging area for multi-national organizations seeking to consolidate data processing arrangements centrally or in a regional hub. The data localization measures found in China’s Cyber Security Law and Indonesia’s Regulation 82 raise specific challenges for those jurisdictions, as does the requirement of an opt-in consent for international transfers from South Korea. Beyond these potential hard stops, the region’s national data protection laws have come into effect, in many cases, with cross-border transfer restrictions in place that will typically allow for a range of compliance measures be taken, whether obtaining data subject consent, imposing contractual restrictions on transferees or exporting to a jurisdiction appearing on an official “white list”.

The APEC Cross-Border Privacy Rules (“APEC CBPR”) system was endorsed in 2011 as a development of the APEC Privacy Framework having an aim of alleviating these concerns. It is a voluntary, principles-based privacy code of conduct for data controllers in participating APEC member economies, based on the nine APEC Privacy Principles developed in the APEC Privacy Framework.

Recent years have seen the APEC CBPR gain momentum, with Australia announcing its intention to become the sixth country to participate in the system (alongside Canada, Japan, Mexico, United States, and South Korea). Additional participating economies are likely to follow, with the Philippines, Singapore and Taiwan having already announced their intention to participate.

Organizations within these economies seeking certification under the APEC CBPR must have their data protection practices and procedures assessed as compliant with the program requirements by an APEC-recognised “Accountability Agent” in the jurisdiction in which they have their principal place of business (their “home” jurisdiction). Personal data from across the participating APEC membership may flow to the organization under the certification, subject to oversight by the Accountability Agent (which would have recourse by law or contract) and home privacy enforcement authority or the privacy enforcement authority in another participating jurisdiction (directly or through co-operation with the home jurisdiction authority).

However, it is important to be clear on the intended scope of the scheme, and its limitations. The CBPR scheme relates only to cross-border data flows. CBPR certification is a badge of compliance against the APEC Privacy Principles, but it does not represent compliance with applicable local privacy laws, so while participating economies recognize APEC CBPR certification as a means of achieving compliance with international transfer restrictions, the full range of remaining privacy issues still need to be considered by participating organizations in each applicable jurisdiction.

The APEC Electronic Commerce Steering Group (the “ESGC”) met with the European Commission
in August 2017 to begin discussions on recognizing the CBPR System as a certification under Article 42 of the GDPR. The effect of this would be to demonstrate that certified organizations have implemented appropriate safeguards within the framework of personal data transfers to “third countries”. It would not replace the requirement for binding and enforceable contractual arrangements to mandate such safeguards on the recipient of the data, but could represent an important step towards inter-operability.

In a separate move to enhance co-operation between jurisdictions on the subject of data transfer in the region, in 2017 the Asia Business Law Institute’s Board of Governors (“ABLI”) launched a multi-stakeholder Data Privacy Project focusing on the regulation of international data transfers in a selection of Asian jurisdictions. Hogan Lovells’ Mark Parsons is among the group of data privacy experts appointed as a Jurisdictional Reporter to advise on the project.

A set of Jurisdictional Reports was published in 2018. In the second phase of the Project, the Jurisdictional Reporters and the wider Experts Committee will draft recommendations on key issues identified, aiming at a convergence of cross-border data transfer requirements across the region.

What to watch for in 2019

We expect the pace of data protection and cyber security regulatory development to continue during 2019.

Key initiatives to watch for:

• There is much anticipation surrounding the finalization of China’s data export review measures as part of its implementation of the Cyber Security Law. Based on the draft implementing measures published to date, there is an expectation that these measures will provide scope for self-assessment of international data transfers below certain materiality thresholds and that there will be some form of a transition period allowing organizations time to achieve compliance.

• India’s consultation towards a new data protection law will set the stage for this very significant economy asserting its influence on regional policy developments for the first time. However, the draft bill has generated significant debate as to what the right balance is for India between data protection, data sovereignty and the freedom for technological innovation that cross-border data transfers can support.

• The implementation of Japan’s “equivalency” agreement with the EU represents a new approach for APAC to address the complexities of cross-border data transfers from the EU.

As always, we should expect the unexpected. Developments in data protection and cyber security regulation tend to be “event driven”. The APAC region has been seeing its share of hacking and data loss incidents and these will unfortunately continue to be on the rise. With an increasing number of dedicated data protection authorities and greater public awareness of data protection risks, we can expect to see enforcement continue to rise. As APAC economies become increasingly digitalized, most recently evidenced by strong government support for smart city/internet of things initiatives and sector specific initiatives such as moves to open financial institutions’ customer data up to wider sharing (“open banking” and “open data” initiatives more generally), the risk factors will continue to rise.

A proportionate response to these issues will be key for the region’s continued development.
Our Asia-Pacific Data Protection Regulatory Heat Map is a graphic representation of the relative stringency of the various data protection regulatory regimes across the region. The map below compares the various regimes in Asia-Pacific by grading jurisdictions against four criteria:

1) data management requirements; 2) data export controls; 3) direct marketing regulation; and 4) the aggressiveness of the enforcement environment. More challenging jurisdictions are represented as red, with less challenging ones appearing as green.
Individual country spotlights

China

China has witnessed rapid developments in data protection regulation in recent years, although it still lacks a comprehensive cross-sector data protection law. China instead relies on a combination of sector-specific laws, consumer protection laws and cyber security laws to regulate data handling practices, supplemented by a number of non-binding national standards. Abuses of privacy remain stubbornly widespread in China’s massive and increasingly wired economy—a problem which the government is seeking to tackle through enhanced regulation and more stringent enforcement efforts.

China’s controversial Cyber Security Law came into effect on 1 June, 2017 and it has already had a significant impact on data collection and processing practices. The focus here is not specifically on data protection, although the data protection measures found in the law are important. The wider remit of the law, which includes technology regulation, has prompted significant criticism from the international community. Technology companies have expressed concerns that the requirement for businesses in China to adopt “secure and controllable” technologies could exclude foreign products from the market. Companies across a range of sectors fear that the policy direction could force them to establish separate operating platforms in China making use of local technology if foreign technology is incapable of achieving certification.

Critics have also stressed that the law has led to more pervasive cyber surveillance and enhanced online censorship, by requiring network operators to store internet logs for at least 6 months, block the dissemination of illegal content, and provide “technical support and assistance” to the authorities in national security and criminal investigations. Much still depends, however, on the content of the implementing regulations to be issued by the Cyberspace Administration of China (“CAC”).

Given the growing cyber threat globally, the Chinese move towards more rigorous cyber security regulation is, in very rough terms, in line with international trends. However, the specific approach to regulation being taken in China is a clear outlier, primarily for the use of broad and often imprecise terminology and also for the invasive and potentially discriminatory nature of the regulations.

The Cyber Security Law regulates two types of organizations: (i) operators of critical information infrastructure (“OCII”); and (ii) network operators (“NO”).

OCII are not bounded by an exhaustive definition and are ultimately subject to designation by the authorities. The Cyber Security Law outlines the industries (including telecommunications, energy, transport and financial services) and state activities (public services and e-government) that form the law’s focus. Prior to the law’s implementation, the CAC published an “Examination Guideline” that laid out materiality thresholds for designating OCII based on considerations such as the number of users of a particular system or platform or the scale of likely impact resulting from a cyber security breach. This guideline will likely be useful in assessing whether or not a particular organization is an OCII under the law. OCII are subject to extensive technology regulation measures, including an obligation to only deploy network products and services that have completed a national security review. There are also far-reaching cyber security administration and reporting obligations under the law.

NO have a far more open-ended definition, essentially encompassing any organization that operates a computer network in China, even if that system is entirely internal to the organization. A key part of the concern over the expansive scope of NOs relates to the Cyber Security Law’s data export review measure.

Article 37 of the Cyber Security Law states that OCII are required to store personal data and “important data” (i.e., having importance in relation to China’s national security or other state interests) in China unless it is necessary to send that data abroad and a security review has been completed. The draft security review measures published by the CAC in May, 2017 purport to extend the application of Article 37 to NOs.
At the time of writing, the export review measures are still to be finalized, generating considerable uncertainty. Few multi-national organizations would expect to be considered to be OCII, but most organizations with operations in China would expect to fall within the scope of NO, as currently elaborated.

Based on commentary from CAC and those advising the Chinese government on the implementation of the law, at this stage we expect that the security review measure will involve mandatory reviews for OCII, but NOs will be subject to a tiered arrangement in which NOs whose international transfers do not meet certain materiality thresholds will be subject only to a self-assessment process, with reporting to the relevant authorities. Our best information to date is that the materiality thresholds may include international transfers involving:

- personal data of 500,000 or more individuals;
- important data relating to sensitive areas of activity, such as nuclear facilities, bio-chemistry, national defence and military;
- important data relating to critical infrastructure system vulnerabilities and safeguards; or
- other circumstances that are likely to adversely impact national security or other state interests.

If one or more of these thresholds is met, the transfer would be subject to official approvals.

The draft measures indicate that international transfers of personal data will not be permitted in a number of circumstances, including where (in the case of personal data) data subjects have not consented to the transfer or other localization measures apply (such as, for example, the existing localization measures applicable to personal financial information or mapping data).

Significant uncertainty remains with respect to the scope and impact of Article 37. The precise nature of substantive review of international transfers has not yet been clarified, and basic considerations such as the test of “necessity” of a transfer and the criteria for assessing the adequacy of security measures have not yet been specified.

There has been official commentary from the CAC that gives us reason to believe that the official intention is not to, for example, force the Chinese localization of multi-nationals’ internal group systems such as HR and CRM systems, and that few international transfers would be subject to
rejection, but in the absence of finalization of the security review measures, it is difficult at this stage to draw any firm conclusions. At least one draft of the security review measures indicated that there would be an 18 month transition period for Article 37. This too has not yet been confirmed.

Various articles in the Cyber Security Law add to the existing patchwork of data protection measures found under Chinese law, most significantly in the Consumer Law, the E-Commerce Law taking effect on 1 January, 2019 and regulations applicable to the collection of personal data through the internet and telecommunications services.

The data protection measures found in the Cyber Security Law have been linked to a new non-binding data protection standard issued by the Standardization Administration of China (“GB/T 35273-2017”), which came into effect on 1 May, 2018. GB/T 35273-2017 provides a series of best practices for the collection, retention, use, sharing and transfer of personal information and for the handling of information security incidents. The standard repeats much of what is already stated in the Cyber Security Law and other laws applying data protection measures (and the earlier non-binding national standard GB/Z 28828-2012), but does add some important new insights and additional glosses on expected best practice:

- a definition of explicit consent (required where sensitive personal data is collected), which includes: (i) a written statement (whether through physical or electronic media), (ii) a ticked box, (iii) registration, (iv) sending a consent message, or (v) the data subject continuing to communicate with the organization collecting the data (a form of implied consent);
- a requirement that encryption be applied to the transmission of sensitive personal data;
- a requirement that when collecting personal data indirectly, the data controller should: (i) require the third party providing the information to explain the source of the personal data; and (ii) investigate whether or not the third party obtained data subject consent to the sharing of their data;
- a requirement that when personal data is transferred as part of a merger, acquisition or restructuring transaction, the data controller must notify the data subject of this fact and the successor to the controller must assume the obligations and responsibilities of the original controller; and if the purpose of use of personal data is changed post-transaction, the successor must obtain a new explicit consent from the data subject; and
- a requirement that data controllers formulate a contingency plan for security incidents that involve personal information and conduct emergency drills at least once a year.

GB/T 35273-2017 is currently under review by the authorities, and we can expect amendments to be made in the course of 2019. We expect to see many of the remaining uncertainties surrounding the Cyber Security Law to come to resolution in the course of 2019.

It is clear that the Cyber Security Law is and will be more actively enforced than existing data protection measures. 2018 saw a consultation on a revamping of China’s Multi-Level Protection Scheme (“MLPS”), which grades organizations on the level of risk arising from their systems, and the introduction of measures providing law enforcement officials with specific powers of inspection in relation to Cyber Security Law Compliance. Enforcement action continues to be significant, particularly with respect to the distribution of unlawful content by internet service providers, but now increasingly in relation to misuse and illegal sales of personal data. References in these enforcement cases to GB/T 35273-2017 underline the importance of this national standard to effective data protection and cyber security compliance for organizations with operations in mainland China.

The regulatory developments in the areas of data protection and cyber security should also be viewed in the wider context of China’s regulation of the internet, which has seen a significant tightening of regulation and administrative practice in recent months. Telecommunications service providers have been ordered to police their networks more closely for usage of unlicensed VPN services and the unlicensed hosting of internet content. The result has been that a number of multi-nationals have had to make adjustments to their platforms and networks in order to meet demands made by their carriers and ISPs. The effect has not been to disable multi-nationals from connecting their Chinese operations to global or regional networks, but the administrative action in recent months has underscored the seriousness with which China is pursuing its cyber space sovereignty agenda.
Hong Kong

Hong Kong’s Privacy Commissioner for Personal Data (the “PCPD”) remains a policy-making leader in the region.

Hong Kong has one of the region’s best developed data protection laws, with the Personal Data (Privacy) Ordinance dating back to 1995.

The PCPD pursues an active agenda of public education and the publication of compliance guidance, including a strong focus on technology related issues.

The PCPD is also closely monitoring the implementation of the GDPR, stating that Hong Kong must “consider the need to establish a comparable framework and mechanism interoperable with international data protection authorities without compromising economic and technological development.”

The PCPD reported a surge of more than twenty percent in the number of data breach notifications made during 2018. This increase came notwithstanding the fact that Hong Kong lacks a mandatory data breach notification obligation. A number of significant and high profile data breaches in the course of 2018, including a reported hacking of a leading Hong Kong-based airline and a consumer credit reporting service, kept data protection in the headlines through much of the year, setting the stage for legislative reform in the course of 2019.

Japan

Japan’s Act on the Protection of Personal Information (“APPI”) dates back to 2003 and so stands as one of Asia’s oldest laws in this area. In the wake of a series of high profile data security breaches and revelations of unlawful sales of personal data in Japan, the Japanese government passed extensive reforms to the APPI taking effect in May, 2017, including:

• the appointment of an independent, dedicated data protection regulatory authority;
• the expansion of the definition of “personal data” to include biometric data;
• the introduction of a concept of “special care-required personal information” (i.e. the concept of “sensitive” personal data) that will be subject to enhanced protections;
• the introduction of restrictions on cross-border transfers of personal data, which will now require: (i) data subject consent; (ii) export to a jurisdiction having the benefit of an adequacy finding; or (iii) satisfaction of other criteria to be specified by the new regulatory authority, including certification under the APEC CBPR program, which Japan; and
• the introduction of data anonymization regulations that will require organizations making use of anonymized personal data to publicly announce the items of data being anonymized and establish internal and external rules for managing “re-identification risk”: i.e., the risk that the data is processed in such a way as to enable the identification of anonymous data subjects.

Japan’s move to modernize its data protection regime has occurred in parallel with its progress towards an Economic Partnership Agreement with the European Union, now concluded, which includes an “equivalency” arrangement under which Japan will amend its laws to impose European standards on personal data imported to Japan from the EU.

Singapore

Singapore has seen a number of recent regulatory developments and the Personal Data Protection Commission (the “PDPC”) has continued to be active in publishing commentary and guidance for businesses and consumers alike.

Singapore’s Cybersecurity Bill was passed into law on 5 February 2018, providing a framework for the regulation of providers of Critical Information Infrastructure (“CII”). The Cyber Security Agency of Singapore will define CII on a sectoral basis. Owners of CII are required to take certain protective measures and comply with reporting requirements, and are ultimately responsible for the security of their CII. This will not extend to multinationals with Singapore offices which are supported by infrastructure located overseas.

The PDPC is in the process of reviewing the Personal Data Protection Act (the “PDPA”) through a public consultation, considering two significant changes to the existing framework. One is the implementation of a mandatory breach notification regime, and the other is the relaxation of the consent requirements on data controllers prior to processing personal data, including where the individual has been notified of the purpose of processing and it is not expected to have any adverse impact on the individual. In practice, it
could be that a notification could be achieved by a disclosure on an organization’s website, but the parameters of this are not yet clear – for example whether there would be limitations as to what the purpose could be, or what recourse an individual would have in response to a notification it does not approve.

The Public Sector (Governance) Bill was passed on 8 January 2018, providing a framework for data sharing arrangements among government agencies. It provides scenarios where such data sharing is permissible in pursuit of certain legitimate objectives, subject to obligations of confidentiality arising from legal privilege or contract. The Bill includes fines or imprisonment terms for unauthorised disclosure and improper use of information.

As is the case in most other jurisdictions, Singapore experienced significant data security breach incidents in the course of 2018, in particular the theft of non-medical personal data of some 1.5 million patients from the SingHealth system. A separate incident involved the disclosure of individuals on the health ministry’s HIV-positive register.

**Australia**

After a lengthy delay, the Privacy Amendment (Notifiable Data Breaches) Act 2017 came into force in Australia on 22 February 2018, requiring that the regulator and impacted data subjects are notified of data breaches. The NDB scheme applies to all agencies and organizations with existing personal information security obligations under the Privacy Act 1998, meaning those with an annual turnover of more than A$3 million, but also applies to certain organisations not meeting this threshold that handle sensitive personal data, such as healthcare providers, and credit reporting bodies. The amended law mandates quick assessment of a suspected data breach to determine whether it is likely to result in serious harm and as a result require notification. Figures published by the Office of the Australian Information Commissioner show a steady pace of notifications being made, with over 800 being reported from the commencement of the regime on 22 February, 2018 through to year end.

The Australian government’s “open data” initiatives have come under scrutiny from a privacy perspective, with comment that privacy safeguards and data anonymity have not been appropriately implemented. Statistics on areas of public interest including on healthcare and crime are being
released as part of the initiatives, but there are concerns that so-called “anonymised” data sets have not in fact been appropriately protected from re-identification risk.

Following a consultation process in 2017, the Australian government commenced participation in the APEC CBPR in November, 2018.

South Korea
South Korea has firmly established itself as one of the toughest jurisdictions for data protection and privacy compliance in the world. Provisions of the over-arching Personal Information Protection Act and the IT Network Act are supplemented by sector-specific laws, creating a very difficult compliance environment. It is noteworthy that the standard for data breach notification under the IT Network Act is understood to be a “leakage” standard under which any unauthorized disclosure of personal data is considered a notifiable breach (as opposed to “harm-based” standards which trigger notification obligations on in circumstances where there is a realistic prospect that harm will come to impacted data subjects due to the breach).

Vietnam
Vietnam’s new Law on Cybersecurity ("Cybersecurity Law"), effective January 2019, has garnered much attention due to its sweeping attempt to regulate online content available to internet users in Vietnam. Among provisions most concerning to multi-national businesses is the requirement that both foreign and domestic online service providers store personal data of Vietnamese end-users in Vietnam, surrender such data to Vietnamese government authorities upon request, and supervise user posts and remove “prohibited” content (defined to include content viewed as disparaging of the Vietnamese government and/or government officials or state agencies). The law also requires offshore service providers to open branches or representative offices in Vietnam, and meet certain data localization requirements, presumably to facilitate enforcement of the Cybersecurity Law against them.

While most foreign companies have elected to take a “wait and see” approach pending issuance of further implementing guidance by relevant agencies, Vietnamese authorities wasted no time in flexing their muscles under the new law by announcing just days after implementation a view that an international social media platform had violated applicable regulations on content control, online advertising and tax liability. However, it
is not entirely clear how the authorities intend to enforce the Cybersecurity Law against foreign service providers without a local presence in Vietnam, nor is it clear what means the government has at its disposal to force foreign providers to actually comply with a request by the authorities that an organisation establish a presence in Vietnam. Practical impacts of the Cybersecurity Law can be expected to play out in 2019.

Thailand
Thailand has had a tortuous journey towards comprehensive data protection regulation. A draft data protection law approved by the Cabinet of Thailand in 2015 was withdrawn, with a new bill introduced in May, 2018. This draft too was replaced by a new bill in September, 2018, which introduced a number of GDPR-inspired concepts, such as the duty to appoint a data protection officer and a right to data portability. The new law adopts extra-territorial effect in a manner similar to the GDPR and imposes an obligation on offshore “data controllers” to appoint a local representative in Thailand. This law appears now to be set for implementation in the course of 2019.

The Philippines
The Philippines’ first comprehensive data protection law, the Data Privacy Act of 2012 (the “DPA”), took effect in September 2012, but it was not until March 2016 that the National Privacy Commission (“NPC”) (the body responsible for enforcing and monitoring compliance with the DPA) was formed. The NPC’s implementing rules and regulations (the “IRRs”) came into effect in September 2016, giving specific meaning to the general requirements of the DPA.

It is fair to say that the IRRs represented a striking move forward for Asia-Pacific data protection laws. Some of the key features of the IRRs are:

- Consent, accompanied by data subject disclosures, is required for any private sector data sharing, and a form of data sharing agreement must be entered into with any transferee. These agreements are subject to review by the NPC;
- The IRRs require that organisations appoint a data protection officer or other person accountable for ensuring the protection of data privacy and security; and
- When data processing is outsourced, the personal information controller must use “contractual or other reasonable means” to ensure that proper safeguards are in place to protect personal data. The IRRs specify the types of clauses that are required in outsourcing contracts with personal information processors.

The most overt borrowings from the GDPR found in the IRRs are a 72 hour data breach notification requirement, data subjects’ right to be informed of profiling and automated decision-making and a right to data portability.

There is also a requirement for personal information controllers and personal information processors to register their data processing systems in certain higher risk scenarios prior to the phase 2 deadline of 8 March 2018.

With the implementation of the IRRs, the Philippines has now set one of the highest bars for data protection compliance in the Asia-Pacific region.

Indonesia
Indonesia has yet to adopt a comprehensive data protection law, but amendments to Government Regulation No. 82 of 2012 regarding the Provision of Systems and Electronic Transactions have introduced a measure of data protection regulation to the country, with multi-nationals paying particular attention to the data localisation measures which came into effect during 2017. Regulation 82 threatens the continued use of regional operating platforms that have, to date, tended to host Indonesian data processing operations in jurisdictions such as Singapore, where a more advanced data centre and telecommunications sector can be found.

With a population of over a quarter billion and one of the highest economic growth rates globally, Indonesia is an increasingly important target for multi-national businesses. Foreign access to this market is being challenged by an increasingly restrictive regulatory environment for data and technology.
Data Protection and Cyber Security regulation in APAC:

A guide to making (and keeping) your business compliant

The tightening of the APAC region’s data protection regulatory environment and the emergence of cyber security regulation comes at the same time as personal data has developed into an increasingly valuable business asset. It also comes as regional businesses seek to turn more to mobile and cloud based operating platforms and transfer data across borders with a view to improving operational efficiency and leverage economies of scale.

An effective data protection and cyber security compliance program begins with a comprehensive look at the personal data being used within the business and then proceeds to map applicable regulatory requirements to this processing.

At a high level, the steps towards developing an effective compliance plan are as follows:

- What personal data does the business hold and use, how was it obtained and for what purposes is it being processed?
- Is the data being transferred to any other group companies or to unrelated third parties for any purpose? If so, into which jurisdictions is the data being sent?
- What future plans does the business have for processing data, in particular having regard to new business lines, new jurisdictions, new technologies, new business models and other potential new avenues to monetising data?
- What data protection and cyber security regulatory regimes apply to the organisation’s personal data holdings, bearing in mind both the location in or from which the data was collected and the location or locations where it is being processed?
- Are the business’s existing policies and procedures compliant? Where are the gaps and what are the practical options for achieving compliance?

Each of these steps is explored in more detail below.

**A Personal Data Audit**

The first step towards developing an effective compliance plan is to understand what personal data the business uses.

**Customer Data**

Customer databases are one of the more obvious holdings of personal data, particularly for consumer facing businesses. The practical issue for identifying the full extent of an organisation’s customer data holdings is that databases are not always clearly marked out as such, particularly now in the era of cloud computing and widespread use of mobile devices.

Engaging with sales, marketing, business development and technology teams is often the key to successfully auditing customer data holdings. Care needs to be taken to understand the specific technologies being used by the business and whether data is being collected or extracted online or through mobile handsets, whether directly or through third party service providers.

Data that has been anonymised or aggregated for profiling or analytics purposes may not, strictly speaking, be “personal data”, but this data should nevertheless be included as part of the audit. Data protection laws generally look at data from an entity-wide or group-wide perspective, meaning that de-personalised data sets that can be linked to identities will not avoid compliance requirements. With the proliferation of social media and online public data sources, the risk of “re-identifying” individuals from anonymised or aggregated datasets has never been higher. Assessing data protection compliance will involve assessing the procedures for creating and maintaining the de-personalisation of these datasets.

**Employee Data**

As Asia region businesses grow in scale and geographic reach, we see a trend towards increased consolidation of human resources databases and increased use of external service providers to administer HR processes and procedures. This development has been running up against
stricter data privacy laws in general and, in particular, the imposition of data export controls in a number of jurisdictions – hence the need to be more vigilant and ensure that data holdings have been properly identified and audited.

An important aspect of employee data is that it almost invariably includes “sensitive personal data” such as information about health and ethnic background. Sensitive personal data is subject to enhanced privacy protection under most of the region’s comprehensive data protection laws and in jurisdictions where it is not subject to explicit enhanced protected (such as Hong Kong and Singapore), data security obligations will nevertheless be proportionately higher in respect of these data.

**Other Personal Data**

Many organisations will also hold personal data about individuals who are not their direct customers, such as shareholders, directors and company officers of corporate customers and suppliers, as well as family members and other individuals who are connected to customers or employees. In the context of social media and cloud services businesses, there are often holdings of user contacts or “refer a friend” data that has not been directly obtained from the business’s customers. This personal data will nevertheless be subject to regulation.

It can very be important to identify data holdings of individuals of this type, given that the business may not have any direct contractual relationship with the individuals concerned, and so find it more challenging to obtain data subject consents and otherwise be sure that compliance requirements have been met.

**Assessing the Means of Collection and the Purposes for Processing**

Once the various personal data holdings within an organisation have been identified, the next task will be to identify how the data was obtained and the purposes for which each group of data is being processed. This will likely again be a matter of engaging with appropriate individuals within functions such as sales and marketing, HR, technology and operations who understand the business processes involved.

As noted above, the pace of technology deployment within an organisation may well run ahead of the legal and compliance teams’ immediate understanding of what sort of collection and
processing is taking place across the business. Data analytics, for example, is an increasingly valuable business tool across a wide range of industries. It is too often the case that these technologies have been deployed without proper compliance checks. As organizations increasingly move to e-commerce and social media platforms to market and sell their products, collecting, sharing and processing personal data through these “ecosystems” requires careful scrutiny, particularly as increased regulatory focus comes to these platforms in the EU and other jurisdictions.

Another area that can raise difficulties is the use of publicly sourced data. In some jurisdictions, such as Singapore, privacy laws do not in general apply to publicly sourced data. In others such as Hong Kong, regulators have made clear that publicly available data may only be used in compliance with general data privacy principles.

We would recommend a holistic approach to analysing purposes be applied, with references to appropriately stress-tested checklists. New purposes for processing data may develop unexpectedly. For example, it may be a rare occasion that a business has a need to consolidate data on the servers of an e-discovery service provider as part of multi-jurisdictional litigation, but it is much better to be prepared for such an eventuality if it is a practical possibility. Likewise, if personal data may be subject to demands by foreign regulators, care will need to be taken to understand this risk in order to factor in appropriate data subject consents and policies and procedures around data handling if the business is in the position to make the disclosure.

Mapping Data Transfers
A related task in the fact gathering process is to understand where personal data is being transferred to from its points of collection, both in terms of transfers to entities within the wider business group and transfers to unrelated third parties. The geographic transit of personal data will also be important given the proliferation of data export controls across the APAC region and the introduction of localization measures in some jurisdictions.

Data transfers can broadly be of two types – (i) transfers to affiliated companies and business partners who collaborate in determining the purposes for data processing or have the discretion to pursue different purposes of processing data (i.e., “controller to controller” transfer scenarios); and (ii) “controller to processor” scenarios in which the transferee simply processes the data in accordance with the transferor’s instructions with no discretion to pursue new purposes for processing.

Both types of transfer will be relevant, although the compliance requirements will differ significantly in each case.

Data Maintenance and Retention
Databases constantly evolve through their use, and so an understanding of how a database is updated, corrected and augmented is key to an effective regulatory analysis.

As the APAC region’s data protection laws are generally consent-based, a key consideration is what procedures are in place to ensure that requests from data subjects that processing cease are appropriately addressed.

Similarly, many of the regimes across the region have express data subject access and correction rights. Businesses will be expected to have policies and procedures in place to manage these requests.

As a general rule, the APAC region’s laws also oblige businesses to cease processing personal data once the purposes for which it has been collected have been exhausted. There are few prescriptive data retention periods under general purpose data protection laws, but businesses will need to undertake an appropriate analysis to determine how long data should be kept. Likewise, it will be important to evaluate approaches to securely erasing personal data once the purposes for having it have been fulfilled.

An Eye to the Future
While much of the personal data audit process is a forensic one aimed at generating a clear snapshot of the current state of data process across a business organisation, a well-executed review will also consider planned extensions of the purposes for processing of data and changes to business operations, such as plans to consolidate databases and deploy new technologies, such as the introduction of remote access by employees to cloud based services, the “bring your own device” policies and the introduction of behavioural profiling technology to company web sites and apps.

Assessing Regulatory Requirements
Once the organisation’s personal data holdings and processing have been understood as a factual matter to a sufficient level of granularity, an analysis against applicable data protection and cyber security regimes can be undertaken.
1. **Leveraging what’s already there**

The regulatory analysis will not necessarily be a matter of re-inventing the wheel, in particular for EU-based multinationals who have invested years of effort in constructing policies and procedures that meet European standards. European standards often (but do not always) meet or exceed national requirements across many jurisdictions in the APAC region, and so it is often efficient to leverage global or regional policies from elsewhere in the organisation if they are transportable having regard to the nature of the business and the data processing taking place. As the APAC region’s data protection and cyber security regimes proliferate and develop, however, there are more and more local distinctions that will need to be taken into account.

2. **A regional approach to compliance**

Irrespective of the starting point a business finds itself in, we generally counsel clients with regional footprints to take a regional view of the APAC region’s data protection and cyber security compliance requirements. With the introduction of the GDPR in 2018, many organizations have started a “global upgrade” of their data protection compliance programs. However, simply rolling out an EU-based compliance program in the APAC region will likely represent “over compliance” in a number of areas. Our recommended approach is to carefully distinguish where the GDPR applies (and where it does not) and craft an efficient compliance solution that involves consistency of approach with EU standards, where appropriate, but fixes a general “APAC standard” that applies with limited exceptions across the region.

“Levelling up” to the “APAC standard” in jurisdictions without data protection laws often makes good business sense, given the obvious trend towards comprehensive regulation across the region. We expect, for example, new laws to emerge in Indonesia and Vietnam in the coming years, and it is a virtual certainty that the new national laws there will take approaches to regulation that are similar to that taken by their neighbours.

There is also, of course, good business sense in having a strong brand for data privacy wherever the business may be. In the area of electronic and mobile commerce and payments, borderless data transfers, cloud computing and remote access to databases, a global or regional approach to managing data security and data privacy is becoming increasingly a business necessity.

While the APAC region has a number of jurisdictions that are yet to implement comprehensive data protection legislation, the region also has a number of jurisdictions sitting at the other end of the compliance spectrum. South Korea, for example, has marked itself out as being one of the world’s most challenging jurisdictions for data privacy compliance. There are other challenges across the region, such as Hong Kong’s
direct marketing controls and Indonesia’s data export requirements. China raises a unique overlay of difficult laws and regulations that pose compliance challenges on a number of fronts and, more recently, the introduction of the Cyber Security Law. The “new normal” for APAC region data protection compliance is setting an ever increasing bar for compliance.

3. Cyber security regulation: ready to respond

Cyber security regulation is steadily introducing new variables to approaches to data management in the APAC region. The introduction of a comprehensive Cyber Security Law in China is an important development. Indonesia’s Regulation 82 is forcing the same considerations there. India’s draft data protection legislation contains a similar measure, allowing onshore-offshore “mirroring” in the main but requiring localization in specific cases.

These developments notwithstanding, cyber security regulation is still at an early stage of development in the APAC region and currently tends to focus only on regulated industries and critical infrastructure. Organizations focusing on cyber security will of course see it as an aspect of data protection (and potentially cyber security) compliance, but more fundamentally it is a matter of business risk across a range of risk areas: in particular operational, financial and reputational.

As data security breaches become more and more commonplace, and increasingly damaging to businesses, we see organizations moving towards greater formality in their cyber security preparations, including through undertaking detailed threat assessments, implementing preventive measures and preparing and testing incident response plans.

Typical Compliance Considerations

The typical range of compliance measures that most businesses will need to turn to will include:

- **Personal information collection statements (PICS)** prepared either as consents or notifications, as applicable, incorporated into customer terms and conditions, privacy policies for web sites and apps, employment terms and conditions and other interfaces with data subjects.

- **Data processing policies and procedures** for internal stakeholders to understand and administer, including policies and procedures dealing with:
  - Data collection and capture, including policies concerning the use of appropriate PICS and the mechanics of collecting consents and the usage of third party data sources;
  - Direct marketing, including alignment of PICS with direct marketing activities, implementation of “opt in”/“opt out” mechanisms, prior consultation with applicable “Do Not Call” registries and compliance with direct marketing formalities, such as consumer response channels and any required “ADV” indicators;
  - Human resources management, including policies dealing with job applicant data, retention of and access to employee files, notification and consent to data privacy policies, employee monitoring, management of sensitive employee data and the use of external vendors for functions such as payroll and counselling;
  - Data analytics, including policies specifying the types of profiling data that may be used, anonymisation/aggregation principles and policies around “enhancing” datasets through the use of publicly available data or third party datasets;
  - Data commercialisation, which looks more broadly for the potential use of the organisation’s data to collaborate with other businesses in marketing initiatives and consumer profiling;
  - Security, including technical standards applicable to various types of internal and external data processing, data access and permissioning, the use of encryption technologies and policies around the use of data in cloud services and other technologies;
  - Business continuity and disaster recovery, including data back-up procedures, the use of redundant storage and contingency planning;
- Data subject access, including procedures for assessing and verifying requests, considering the legal implications of requests and managing costs of responding to requests;

- Complaints handling, including complaints from customers, employees and other affected individuals;

- Data quality management, including procedures for updating and correcting databases and determining if data is to be erased;

- Data processing and outsourcing, including vendor due diligence policies and standard contract clauses and templates for onshore and offshore processing, addressing both data protection and cyber security concerns;

- Data retention, including policies for determining how long data of various types are to be retained and how it is to be securely destroyed;

- Cyber threat assessments and incident response planning, including programs to identify and review cyber threats across the organisation, allocation of responsibilities for escalation of and response to incidents;

- Data breach management, including policies for escalating, containing and remediating data breaches and evaluating the need for regulatory or data subject notifications, as well as procedures for assessing any need for change to policies and procedures following the occurrence of a breach; and

- Privacy impact assessment, which includes a general framework for the organisation to assess privacy impacts due to proposals for organisational, technological or policy change.
Management oversight and review
Developing effective data protection and cyber security risk management policies and programs will involve engagement with the right stakeholders across the organisation and creating an effective governance regime for approving, overseeing, implementing and reviewing the various policies. The appointment of official roles such as a Data Protection Officer is becoming more common as best practice in the region, even in jurisdictions where the designation is not required by law.

Regulators in the region are becoming increasingly conscious of the degree to which data protection and cyber security policies have been prepared under senior management and board direction. Input from such high levels lends credibility to the compliance effort. Effective implementation of data privacy policies will need to consider appropriate channels for reinforcement of new policies following their publication. Training of individuals within the organisation will be necessary in order to lend context and emphasise the importance of compliance to the business. The policies will need to be seen to have been acted upon in order to be evidence of due compliance, and so enforcement procedures will be critical. Policy breaches will need to be examined after the fact with a view to understanding whether or not any organisational change is needed in response.

In order to be effective, an organisation’s data privacy policies will need to be under regular review, reflecting changes in law and regulation, changes in the data being collected and used and changes in technologies and operating procedures. The benefit of experience must also be brought to bear.
Our APAC data protection and cyber security practice

An international perspective

At Hogan Lovells we bring an international perspective to advising clients on the APAC region’s data protection and cyber security laws and the ongoing development of policy across the region. Our APAC region team includes practitioners who practised data privacy law in Europe, and so bring a depth of experience to interpreting APAC region laws that have a common origin in the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. At the same time, our experts are on the ground in the region and rooted in the local law and language, sensitive to the important emerging local nuances.

Integrated support

Our APAC region team is closely integrated with our international team of data protection and cyber security practitioners, and so benefits heavily from a wider team of market-leading lawyers who are at the forefront of policy developments in Europe and the United States, advising clients on the most critical mandates on a world-wide basis.

Where Hogan Lovells does not have offices in the APAC region, we have strong working relationships with local counsel experts. These relationships have developed over the course of the effective lifetime of these emerging laws, supporting the delivery of a uniformly consistent and high quality work product and practical solutions for business.

Our APAC region data protection and cyber security team is also closely integrated with other relevant specialists, in particular lawyers engaged in commercial arrangements concerning data commercialisation and processing and employment law specialists. Our seamlessness on this front means that we bring a very practical, solutions-based approach to counselling that is well informed by market practice.

Key points

Our advice covers all aspects of data protection and cyber security compliance, including:

- Conducting data protection and cyber security compliance audits and developing policies, including integrating Asia policies with existing international policies;
- Helping clients structure and allocate risk in relation to cross-border data transfers, including as part of outsourcing, shared services and cloud arrangements;
- Advising on the acquisition of personal data as an increasingly important part of merger and acquisition and joint venture activity;
- Advising on data protection issues arising from online data capture, whether as part of electronic and mobile commerce, behavioural profiling or otherwise;
- Advising on commercial arrangements, such as marketing, distribution and sponsorship agreements, where securing rights to use personal data is a key business objective;
- Advising on cyber-security regulation and cyber-readiness planning;
- Advising on data breach notification requirements when data is hacked or lost;
- Advising on data subject access requests;
- Defending companies against enforcement actions; and
- Bringing to bear the knowledge and experience of our extensive and market-leading data protection and cyber security management team across the world in finding solutions that work in Asia based on lessons learnt elsewhere.
Key Contacts in APAC

**Hong Kong**

Mark Parsons  
Partner  
T +852 2840 5033  
mark.parsons@hoganlovells.com

Eugene Low  
Partner  
T +852 2840 5907  
eugene.low@hoganlovells.com

Tommy Liu  
Senior Associate  
T +852 2840 5072  
tommy.liu@hoganlovells.com

**Shanghai**

Philip Cheng  
Partner  
T +86 21 6122 3816  
philip.cheng@hoganlovells.com

Andrew McGinty  
Partner  
T +86 21 6122 3866  
andrew.mcginty@hoganlovells.com

**Beijing**

Jun Wei  
Partner  
T +86 10 6582 9501  

Roy Zou  
Partner  
T +86 10 6582 9488  
royzou@hoganlovells.com

Sherry Gong  
Counsel  
T +86 10 6582 9516  
sherry.gong@hoganlovells.com

**Japan**

Hiroto Imai  
Partner  
T +81 3 5157 8166  
hiroto.imai@hoganlovells.com

**Singapore**

Stephanie Keen  
Partner  
T +65 6302 2553  
stephanie.keen@hoganlovells.com

**Vietnam**

Jeff Olson  
Partner  
T +84 8 3825 6370  
jeff.olson@hoganlovells.com
Our global Privacy and Cybersecurity practice

Realizing the true value of data
Finding the right balance between the most fruitful use of data and the protection of privacy is one of the greatest challenges of our time. Personal information is an extremely valuable asset and its responsible exploitation is crucial for the world’s prosperity. For that reason, our approach is to look at privacy compliance and information governance as part of our clients’ strategic vision for success.

Embracing privacy, data protection, and cyber security can be crucial in order to gain competitive advantage, because it will promote employee and customer loyalty, encourage consistency and efficiency, and facilitate international expansion. In addition, we believe that privacy is not only compatible with innovation, but can make a valuable contribution to it.

With its depth of knowledge and global presence, Hogan Lovells’ Privacy and Information Management team is uniquely placed to help clients realize this potential. We have extensive experience of assisting clients with multi-jurisdictional projects and understand the complexities involved in dealing with laws and regulators across the world.

What we offer
- A true specialist practice focused on privacy, cyber security, data protection, and information management
- Thought leadership and close involvement in the development and interpretation of the law
- Seamless global coverage through our well established and continuously developing team
- Advice which goes beyond achieving compliance and adds value to the information held by organizations
- A one stop shop for all of your data privacy needs around the globe.

Our focus and experience
The Hogan Lovells Privacy and Cybersecurity practice spans the globe and all aspects of privacy, data protection, cyber security, and information management.

- No other team in the world has our track record of BCR approvals. We have advised on and successfully secured approvals of BCRs for nine applicant companies and are currently working on several BCR projects.
- We have worked with numerous multi-nationals on other data transfer solutions, including adoption of model clauses, intra group agreements and Safe Harbor.
- We have advised numerous global companies with respect to complying with their notification obligations across the EU.
- We have drafted and advised on many global data processing contractual arrangements to ensure practical and effective compliance with security related obligations.
- We have liaised with policy makers throughout the world and contributed to the legislative process in the EU and other jurisdictions.
- We have assisted clients in devising and implementing regulator cooperation strategies, including liaising closely with EU data protection authorities.
- We have surveyed in detail the laws and regulations impacting employee monitoring practices in over 60 countries, including important markets in Europe, the Americas, Asia, the Middle East and Africa.
- We advised a number of global companies on data privacy questions arising from their migration of HR and customer data of their European subsidiaries to cloud service providers.
- We have advised many multi-nationals on localising website privacy policies.
- We have assisted leading global companies to adopt and implement a pan-European strategy in respect of the EU cookie consent requirements for their website and mobile application offerings.
- We provided strategic advice to a number of clients on data breach notification requirements throughout the world.
- We have advised on complex matters ranging from the use of biometrics to the collection of mobile device data, including making submissions to multiple data protection authorities to facilitate the introduction of these technologies into global markets.

**How we can help**

We have had a team specializing in Privacy and Cybersecurity for over 25 years. Today Hogan Lovells has one of the largest and most experienced Privacy and Information Management practices in the world, spanning the United States, Europe, and Asia. We assist clients with all of their compliance and risk management challenges, drafting policies and providing advice on legal issues, risk management strategies, and strategic governance. With our global reach, we are able to provide a 24-hour global privacy hotline to respond to data emergencies. We play an important role in the development of public policy regarding the future regulation of privacy. Additionally, we provide the latest privacy and data protection legal developments and trends to our clients via our blog, **Chronicle of Data Protection** (http://www.hldataprotection.com).