DREW & NAPIER

DATA PROTECTION QUARTERLY UPDATE

March 2016

In this issue

WELCOME MESSAGE

The Drew & Napier Telecommunications, Media and Technology Practice Group is pleased to present the first issue of our Data Protection Quarterly Update.

Every three months, this publication will highlight the need-to-know data protection law developments in Singapore, and in key jurisdictions around the world.

In this issue, we see the emergence of new regulatory instruments and frameworks in APAC and in Europe, as courts, governments, and regulators continue to grapple with rapid advancements in new technologies and their implications on the ways in which personal data can be utilised.

We hope that this new publication will be useful to you, as you navigate the increasingly complex regulatory landscape in data protection law. We welcome your feedback and questions on any of the data protection news and articles featured in this Quarterly Update, as well as any suggestions you may have on topics to be covered in the future.

For more details on the Drew & Napier Telecommunications, Media and Technology Practice Group, please visit: **http://www.drewnapier.com/Our-Expertise/Telecommunications,-Media-Technology**.

IN THE NEWS

SINGAPORE

Formation of the Info-communications Media Development Authority and Government Technology Organisation

On 15 January 2016, noting the convergence of the info-communications and media sectors due to rapid technological advancements, the Minister for Communications and Information (***Minister***) announced in Parliament that the Info-communications Development Authority of Singapore (***IDA***) and the Media Development Authority of Singapore (***MDA***) will be restructured

to form a new info-communications and media regulator, the Info-communications Media Development Authority of Singapore (***IMDA***). As part of the restructuring process, the Government Chief Information Office that currently functions within the IDA will be restructured as an independent entity, the Government Technology Organisation (***GTO***). The Minister noted that these measures will ensure that Singapore remains adaptable to technological developments and advancements, and will be well-placed to seize economic opportunities.

The restructuring follows the launch, in August 2015, of the Infocomm Media 2025 plan, the first integrated industry development plan for the info-communications and media sectors. It also recognises the importance of the digital economy in transforming many sectors of the economy, as well as the need to support the transformation of government service delivery through even more intensive use of Information Technology (***IT***).

In a further speech in Parliament on 26 January 2016, the Minister remarked that info-communications media technologies have fundamentally disrupted established business models. For example, the biggest taxi company in the world, Uber, does not own a single car, and the largest purveyor of accommodation in the world, Airbnb, owns no hotel rooms. Recognising that these changes will only accelerate, the Minister stated that the motivation to restructure the IDA and MDA is to help Singapore seize opportunities presented by technological changes, for example, in the areas of convergence (i.e., the increasing overlap between information and communications technology (***ICT***) and media), Big Data, and the Internet of Things. The Minister also noted that as technology changes and matures, the new GTO will help the Singapore Government understand and use technology boldly to deliver better public services.

Role of new Info-communications Media Development Authority of Singapore

The IMDA will be Singapore's newly converged regulator in the info-communications and media sectors. It will combine the regulatory functions of the IDA, which presently regulates the info-communications sector, and the MDA, which presently regulates the media sector.

In announcing the formation of the IMDA, the Singapore Government expressly recognised that a key driver of the restructuring is the phenomenon of increasing convergence between the info-communications and media sectors, which has blurred the traditional distinction between telecommunications and broadcasting. The newly converged regulator, IMDA, is expected to develop and regulate the converging info-communications and media sectors in a holistic way. In this regard, the IMDA will be expected to:

(a) spearhead the Infocomm Media Masterplan 2025;

(b) oversee policy formulation for the converged environment;

(c) deepen regulatory capabilities for a converged infocomm and media sector;

(d) safeguard the interests of consumers; and

(e) foster pro-enterprise regulations.

The Minister has also announced that the Personal Data Protection Commission (***PDPC***) will be incorporated into the new IMDA, in order to bring about better policy synergy. The PDPC is the authority responsible for administering and enforcing the Personal Data Protection Act 2012 (***PDPA***), which establishes Singapore's general data protection law. With increasingly pervasive use of data, the Singapore Government will continue to promote and regulate data protection in Singapore through the PDPC. This will ensure that public confidence in the private sector's use of personal data is safeguarded, even as companies increasingly leverage the data they collect as a source of competitive advantage.

Role of new Government Technology Organisation

The GTO will include all the functions of IDA's Government Chief Information Office in providing enterprise IT solutions to over 90 Government agencies, governing ICT standards within public agencies and coordinating the three-year ICT masterplans across Government for more effective procurement of ICT services.

As the Singapore Government continues to adopt new and emerging technologies for better service delivery, the GTO will be expected to safeguard Government digital services against cyber threats. Further, the GTO will be expected to provide robust and cyber-resilient information technology services for the Government.

With an expanded mandate to grow new technology capabilities, the new GTO will lead

digital transformation efforts in the public sector. The GTO is expected to help government agencies capitalise on the speed of innovation and new technology trends such as robotics, artificial intelligence, Internet of Things, and Big Data. Further, the GTO will also play a vital role in supporting Singapore's Smart Nation vision, especially in delivering the Smart Nation Platform and Smart Nation applications. In addition, the GTO will also focus on developing new technology capabilities as well as attracting and nurturing ICT engineering talent that will provide a strong foundation for Singapore's Smart Nation ambitions.

Potential impact on the regulatory framework

The Ministry of Communications and Information (***MCI***) has announced that the IMDA and GTO will be established in the second half of 2016. In preparation for the formal establishment of the two new bodies, the IDA and MDA will be administratively re-organised from 1 April 2016.

The existing regulatory framework, where the IDA and the MDA are presently the regulators for the info-communications and media sectors respectively, are expected to undergo a number of changes. The Minister has stated in Parliament that as a unified authority, the IMDA will be able to enact competition and consumer protection regulations in a more holistic and progressive manner. The Telecommunications Act, Broadcasting Act and Films Act will also be updated to keep pace with the demands of the converged info-communications media space.

The Minister also noted the need to ensure that the Smart Nation initiative is built upon a secure, robust and resilient infrastructure. To this end, a national cyber security strategy will be developed to strengthen Singapore's information infrastructure, and a Cyber Security Bill will be introduced in order to give the Cyber Security Agency of Singapore greater powers to secure Singapore's critical information infrastructure.

MALAYSIA

Personal Data Protection Standard 2015

The Personal Data Protection Standard 2015, which came into force on 23 December 2015, sets out minimum standards that aim to provide guidance in the application of the Personal Data Protection Act 2010. These standards focus on data security, retention and integrity.

Data Security Standard

The Data Security Standard distinguishes between conventional and electronic management of personal data, and requires different security measures to be taken. For example, the security measures proposed for personal data managed electronically include restricted access, password protection, protection against malware and viruses, as well as the implementation of a backup or recovery system to prevent data loss. In contrast, conventional records are required to be kept in an orderly manner under lock and key.

Data Retention Standard

The Data Retention Standard concerns the destruction and deletion of personal data once it is no longer required. For example, the Data Retention Standard contemplates requiring data users to destroy data collection forms and customer data after 14 days unless the data user is legally obliged to retain the same.

Data Integrity Standard

Similar to the Data Security Standard, the Data Integrity Standard also distinguishes between conventional and electronic management of personal data. That said, there are similarities in the proposed steps for both categories of data, which include preparing standard forms to be used for data correction requests, and correcting the data within seven days of receiving a correction request.

In Singapore:

Section 24 of the PDPA requires organisations to make reasonable security arrangements to protect personal data in their possession or under their control in order to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks. The PDPC has also issued a non-legally binding Guide to Securing Personal Data in Electronic Medium to provide information and examples on good practices which organisations may adopt to further secure electronic data. The Guide, which is especially relevant for persons who are responsible for data protection and also persons who supervise or work with information and communications technology systems and processes, provides a consolidated checklist of Good Practices and

Enhanced Practices that are useful for organisations in strengthening their data compliance obligations.

The Accuracy Obligation under Section 23 of the PDPA requires organisations to make a reasonable effort to ensure that personal data collected by or on behalf of the organisation is accurate and complete if the personal data is: (a) likely to be used by the organisation to make a decision that affects the individual to whom the personal data relates; or (b) is likely to be disclosed by the organisation to another organisation. The non-legally binding Advisory Guidelines on Key Concepts in the PDPA clarify that organisations may not be required to check the accuracy and completeness of an individual's personal data each and every time they make a decision about an individual. Rather, organisations should perform their own risk assessment and use reasonable effort to ensure the accuracy and completeness of such personal data that is likely to be used to make a decision that will affect the individual.

The Retention Limitation Obligation under section 25 of the PDPA provides that organisations shall cease to retain documents containing personal data, or anonymise such personal data, as soon as it is reasonable to assume that the purpose for which that personal data was collected is no longer being served by the retention of the personal data, and retention is no longer necessary for legal or business purposes. Although the PDPA does not prescribe a specific retention period for personal data, organisations would need to comply with any legal or specific industry-standard requirements which may apply.

HONG KONG

Office of the Privacy Commissioner for Personal Data (*PCPD*) issues guide on online collection and use of children's personal data

On 1 December 2015, the PCPD issued a guide entitled "*Collection and Use of Personal Data through the Internet – Points to Note for Data Users Targeting at Children*" (***Guide***). The Guide is aimed at data users who interact with children via the Internet, and who are likely to collect children's personal data via online means.

The Guide defines "children" to refer generally to those aged under 18. The Guide recognises children as a "vulnerable group" that has special privacy protection requirements, particularly in the context of online activities.

The Guide includes a number of best practices and other tips for data users, particularly those who operate online platforms, to ensure that they protect and respect children's personal data. The measures suggested by the PCPD relate to the categories of: (a) collection of personal data; (b) use of personal data; (c) security of personal data; and (d) transparency in privacy policy and practice.

The following is a non-exhaustive summary of the measures set out in the Guide.

Collection of personal data

As a starting point, the PCPD suggests that data users consider not collecting any personal data from children altogether (instead of just limiting the collection of personal data).

In the case of data users who use online forms to collect personal data, the Guide states that, as a best practice tip, data users should: (a) use a two-part form to group mandatory and optional fields separately; (b) avoid using open-ended questions in which children may feel inclined to over-supply information; and (c) using "just in time" reminders or warning messages to alert children of the minimum amount of information they are expected to supply.

In the case of data users who collect information about third parties (e.g. parents or friends) from children, the Guide states that, as a best practice, data users should explicitly remind children to consult and obtain consent from those third parties before providing their personal data.

Use of personal data

For data users that operate online platforms, the PCPD suggests that the online platforms' default privacy settings be pre-set with privacy protection in mind. In the case of online platforms that involve the sharing of information between users or members of the public, the Guide states that, as a form of best practice, the default setting for all sharing should be set as restrictive as possible, and there should also be sufficient notice and explanation provided to children on the implications of these privacy settings.

In the case of data users whose online platforms allow or require children to use their social network accounts for interaction (e.g. logging in, using "like", "share" or similar actions that may show the children's social network account names), the Guide states that data users should explain clearly to children the implications of using their social network accounts. As a form of best practice, data users should offer either anonymous log-in or allow children to create separate accounts (instead of requiring or allowing the use of social network accounts) on their online platforms.

In relation to the disclosure of children's personal data, the Guide states that, on online platforms where children's personal data is to be published, data users should provide clear notice to children on or before collecting the data, as well as limit access to those who have a genuine need to access that information. As a best practice, data users should provide children with the means to opt-out of such publication. Data users should also consider using pseudonyms to identify individuals. For example, when data users post participant lists for sporting events, they should use pseudonyms such as participant number, limit the amount of information disclosed, and/or limit the audience that can access the personal data to the smallest group possible. When data users wish to post event photos, they should ensure that all participants are informed of the arrangement before the pictures are taken and, as a best practice, offer an opt-out mechanism.

Security of personal data

The Guide also reminds data users of the need to protect personal data collected, notwithstanding that some online platforms targeting children may be of a social or leisure nature. In this regard, the Guide states that data users must conduct a risk assessment to determine the risk of a security breach and the harm that it may cause.

Transparency in privacy policy and practice

With respect to privacy policies, the Guide reminds data users to keep the target audience in mind in their choice of language and presentation. The Guide states that a privacy policy that is legalistic is unlikely to be understood by children, and in the case of online platforms which target different age groups, data users are recommended to develop different age-appropriate versions of their privacy policy.

The Guide also states that data users should consider providing a single place on their online platform for children to find out what personal data has been collected or maintained. As a best practice tip, data users may provide a "dashboard" for children to see, change and remove all postings (where applicable) and personal data collected. The dashboard may also include all privacy-related settings. Particularly in the case of younger children, data users may extend such dashboards to parents so that they can help younger children to manage their own personal data privacy.

In Singapore:

*The PDPA does not expressly distinguish minors from other individuals. That said, the PDPC has recognised that special considerations may apply to minors, in the context of the PDPA. In its Advisory Guidelines on the PDPA for Selected Topics (**Guidelines**), the PDPC has defined a minor to mean an individual who is less than 21 years of age.*

In particular, an issue which organisations may need to consider, depending on the circumstances of each case, is whether a minor may give valid consent for the purposes of the PDPA.

The PDPC has stated in the Guidelines that, in general, whether a minor can give consent for the purposes of the PDPA would depend on other legislation and the common law – where there is no legislation that affects whether a minor may give consent, the issue would be governed by common law.

In this regard, the PDPC's view is that organisations should generally consider whether a minor has sufficient understanding of the nature and consequences of giving consent, in determining if he can effectively provide consent on his own behalf for the purposes of the PDPA. As a practical rule of thumb, the PDPC will consider that a minor who is at least 13 years of age would typically have sufficient understanding to be able to consent on his own behalf.

Overall, however, organisations should take appropriate steps to ensure that the minor can effectively give consent on his own behalf in the circumstances of the particular case. For example, where an organisation has reason to believe that a minor does not have sufficient understanding of the nature and consequences of giving consent, it should obtain consent from an individual who is

legally able to provide consent on the minor's behalf such as the parent or guardian.

PCPD issues revised Best Practice Guide for Mobile App Development

In October 2015, the PCPD published a revised edition of its Best Practice Guide for Mobile App Development (***Mobile App Guide***).

The Mobile App Guide is targeted at mobile app developers (including those who commission the development of the app or decide on the purpose of the app), as well as those who provide codes to app developers for added features such as advertising networks and analytics tool providers.

The Mobile App Guide seeks to provide practical guidance to mobile app developers in a number of areas, including:

(a) legal requirements under the Personal Data (Privacy) Ordinance;

(b) the "Privacy by Design" approach to protecting privacy (see further below);

(c) a checklist for app development; and

(d) best practice recommendations.

In terms of an approach to app development, the Mobile App Guide suggests that app developers seek to build in privacy protection at the outset of a project, rather than wait until the last stage of the project to adjust for compliance sincethe latter approach would have a greater impact on app functions.

The Mobile App Guide also refers to the "Privacy by Design" approach (**www.privacybydesign.ca**), which emphasises privacy considerations "throughout the entire development life cycle". In this regard, the Mobile App Guide sets out four key areas in which the Privacy by Design approach may be applied to app development, briefly summarized as follows:

(a) **Data minimisation.** Reducing the collection of personal data (particularly sensitive personal data) to the absolute minimum is the key element of Privacy by Design.

(b) **Surprise minimisation.** The PCPD suggests that app developers be open and frank to users on what information would be accessed or used, and to give users the choice to opt-out from such access or use.

(c) **Risk minimisation.** If data is being transmitted and/or stored, app developers would need to put in place adequate protection, in terms of encryption and access control, to ensure that there is no unauthorised access, disclosure or use of their users' personal data.

(d) **Trust and respect.** The PCPD notes that, even if app developers do not think the data their app access/collects can be regarded as personal data, telling app users what data their app accesses or collects will earn the trust of the app users.

The Mobile App Guide also contains a checklist that app developers can use to apply the Privacy by Design approach to their app design.

The PCPD also provides a number of best practice recommendations for app developers, which are grouped under the following broad recommendations:

(a) only accessing or collecting or using data when necessary;

(b) only transmitting or uploading data when necessary;

(c) only storing or keeping data elsewhere from the mobile device when necessary;

(d) only combining or correlating data with other data of the app user obtained elsewhere when it is appropriate;

(e) sharing the data within the business or with other parties only if appropriate;

(f) being transparent if using data for profiling individuals;

(g) obtaining consent from target customers before using their personal data for direct marketing;

(h) being transparent in the Personal Information Collection Statement and Privacy Policy Statement;

(i) taking into account app users' privacy expectations; and

(j) being transparent if using, including or providing third-party app-development tools.

For apps that do not access or collect personal data, the PCPD recommends that app developers should, nevertheless, provide a privacy policy statement to the user.

In Singapore:

App developers in Singapore will, like other organisations, generally need to ensure compliance with PDPA. While the PDPC has not issued a set of guidelines dealing specifically with the development or design of mobile apps, other guidelines issued by the PDPC may be relevant in this regard. For example, the PDPC's Guide to Notification provides brief examples of how notification may be provided to users in the context of mobile apps. The PDPC's Advisory Guidelines on the PDPA for Selected Topics also contains a section pertaining to online activities.

PCPD issues revised guidance on data breach handling

In October 2015, the PCPD published a revised edition of its Guidance on Data Breach Handling and the Giving of Breach Notifications (**Data Breach Guidance**). The Data Breach Guidance describes how data users should react in the event of a data breach.

The Data Breach Guidance defines a data breach generally to be "a suspected breach of data security of personal data held by a data user, exposing the data to the risk of unauthorised or accidental access, processing, erasure, loss or use." Examples include improper handling of personal data and hacking of a database containing personal data.

The Data Breach Guidance highlights that a data breach may amount to a contravention of Principles 4(1) and (2) of the Personal Data (Privacy) Ordinance (***Ordinance***):

(a) Principle 4(1) provides that a data user shall take all reasonably practicable steps to ensure that personal data held by it is protected against authorised or accidental access, processing, erasure, loss or use, having particular regard to the kind of the data and the harm that could result if any of those things should occur.

(b) Principle 4(2) provides that if a data user engages a data processor, whether within or outside Hong Kong, to process personal data on the data user's behalf, the data user must adopt contractual or other means to prevent unauthorised or accidental access, processing, erasure, loss or use of the data transferred to the data processor for processing.

The Data Breach Guidance states that data users shall take remedial actions to lessen the harm or damage that may be caused to the data subjects in a data breach. Specifically, the Data Breach Guidance suggests a four-step action plan, briefly summarised as follows:

Step 1: Immediate gathering of essential information relating to the breach

The Data Breach Guidance recommends that the data user promptly gather the following essential information:

(a) When did the breach occur?

(b) Where did the breach take place?

(c) How was the breach detected and by whom was it detected?

(d) What was the cause of the breach?

(e) What was the kind and extent of personal data involved?

(f) How many data subjects were affected?

The Data Breach Guidance further recommends that the data user consider designating a coordinator (an appropriate individual/team) to assume overall responsibility in handling the data breach incident.

Step 2: Contacting the interested parties and adopting measures to contain the breach

Having detected the breach, the next step would be for the data user to identify the cause of, and stop, the breach. To this end, the PCPD suggests a number of containment measures. For example, the data user may change users' passwords and system configurations to control access and use. The data user may also notify the relevant law enforcement agencies if identity theft or other criminal activities are being, or are likely to be, committed.

Step 3: Assessing the risk of harm

The Data Breach Guidance states that the types of damage that may potentially be caused by a data breach include:

(a) threat to personal safety;

(b) identity theft;

(c) financial loss;

(d) humiliation or loss of dignity, damage to reputation or relationship; and

(e) loss of business and employment opportunities.

The Data Breach Guidance also lists various factors that may contribute to the extent of the harm. The Data Breach Guidance states that, for example, when a database containing personal particulars, contact details and financial data is accidentally leaked online through file-sharing software, an assessment may indicate a real risk of harm. On the other hand, a lower risk of harm may be involved in the loss of USB flash drive containing securely encrypted data which is not sensitive in nature, or when a small number of data subjects are affected, or when a lost or misplaced instrument containing personal data has subsequently been found and the personal data does not appear to have been accessed.

Step 4: Considering the giving of data breach notification

The Data Breach Guidance states that, where the data subjects affected by the breach can be identified, the data user should consider notifying data subjects and the relevant parties when a real risk of harm is reasonably foreseeable.

Data breach notification

While the Data Breach Guidance states that data breach notifications are not required by the Ordinance, data users are encouraged to adopt a system of notification in handling data breaches.

A data breach notification may be given to the affected data subjects, law enforcement agencies, the Privacy Commissioner, relevant regulators, and other parties who may be able to take remedial actions to protect the personal data. For example, Internet search engines may be asked to remove relevant links. The notification should be made as soon as practicable unless law enforcement agencies have requested a delay due to investigative reasons. Furthermore, the scope of the notification should be carefully determined so as to include salient information about the breach without compromising concurrent investigations.

Finally, the Data Breach Guidance recommends that data users take steps to learn from data breaches and avoid a repeat of the breaches.

In Singapore:

Depending on the circumstances, a data breach may (without limitation) amount to a breach of Section 24 of the PDPA. Section 24 of the PDPA requires organisations to protect personal data in their possession or under their control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.

The PDPC has published a Guide to Managing Data Breaches, which includes guidance to organisations on how to respond to a data breach incident. Amongst other things, it recommends that organisations implement a data breach management plan. The plan may include provisions for the following activities: act to contain the breach, assess the risks and impact of the breach, report the incident to relevant parties, and conduct an evaluation to avoid future breaches.

The PDPA does not expressly require an organisation to notify affected individuals or the PDPC in the event of a data breach. That said, the PDPC's Guide to Managing Data Breaches states that, in general, it is a good practice to notify individuals affected by a data breach. The PDPC's website also states that, in the event of a breach, the mitigating factors which the PDPC may consider include: (a) whether the organisation informed individuals of steps they can take to mitigate risk caused by a data breach; and (b) whether the organisation voluntarily disclosed the personal data breach to the PDPC as soon as it learned of the breach and cooperated with the PDPC's investigation.

As such, organisations should ensure they have a plan in place to respond to any data breaches in respect of personal data in their possession or under their control. In the event of a data breach, organisations should consider carefully whether a breach notification should be made.

Organisations should also note that, under the PDPA, an organisation has the same obligations in respect of personal data that is processed on its behalf and for its purposes by a data intermediary, as if the personal data were processed by the organisation itself. As such, organisations which engage data intermediaries to process personal data on their behalf should exercise prudence in ensuring that their data intermediaries are able to satisfy their obligations under the PDPA, and if appropriate, take steps to minimise risks in this regard.

JAPAN

Amendments to Japan's APPI

The overarching legislation governing the protection of personal data in Japan is the Act on the Protection of Personal Information (Act No. 57 of 2003) (***APPI***). The APPI was enacted in 2003 and came into full force in 2005. On 3 September 2015, the bill to amend the APPI (***Amended APPI***) was approved by the Japanese Diet. The date at which the Amended APPI will come into full force has not yet been decided.

The following paragraphs set out a brief and non-exhaustive summary of the key amendments to the APPI:

(a) **Establishment of the Personal Information Protection Commission.** The protection of personal data is currently regulated by different government ministries, which have adopted different guidelines tailored towards the needs of the respective industries that they are in charge of. Under the Amended APPI, the Personal Information Protection Commission ("**Commission**") will bring the separate guidelines into alignment. In addition, the Commission will exercise functions including issuing administrative orders; requesting data controllers to submit reports; and conducting onsite inspections.

(b) **Expansion of the definition of personal information.** The Amended APPI clarifies that the scope of protected personal information includes any "personal identifier code", which refers to any biometric data that identifies a specific individual or any code uniquely assigned to an individual. Such data include an individual's fingerprint data, face recognition data, driver licence numbers and biometric passport numbers.

(c) **Sensitive personal data.** Under the APPI, there is no provision which provides for sensitive personal data even though some of the administrative guidelines for the APPI that are adopted by Government ministries and agencies impose strict restrictions on the collection, use and disclosure to third parties of certain forms of sensitive data. The Amended APPI introduces a provision governing sensitive personal data to include information about a person's race, creed, social status, medical history, criminal record, any crimes that an individual has been a victim of, and any other information that may cause the individual to be discriminated against. Such sensitive personal data are not to be provided by organisations without the consent of the individual and the provision of such sensitive personal data to third parties will be subject to a higher level of scrutiny.

(d) **Anonymised information.** While there is currently no provision providing for anonymised information under the APPI, the Amended APPI will introduce such a provision. Anonymised information may be transmitted without the express consent of individuals, subject to the extent of how thorough an organisation is in anonymizing the personal data before the transmission of such data.

(e) **Cross border transfers of personal data.** Currently, there are no restrictions on transfers of personal data overseas. The Amended APPI provides that organisations transferring personal data overseas are required to undertake certain actions such as entering into contracts to protect the security of personal data. However, organisations do not need to take such actions if the data is being transferred to a country determined by the Personal Information Protection Commission as having data protection standards that are equivalent to Japan; or if a foreign transferee has data protection standards that are equivalent to the standards specified by the Personal Information Protection Commission.

(f) **Criminal sanctions.** Apart from the current criminal penalties and remedial recommendations set out under the APPI, the Amended APPI further provides for criminal penalties in relation to stealing,

misappropriating or supplying personal data for unjust profits.

In Singapore:

Pursuant to section 6 of the PDPA, the functions of the PDPC include administering and enforcing the PDPA.

Apart from not having a provision governing sensitive personal data in Singapore as all forms of personal data, regardless of the degree of sensitivity, are covered under the PDPA, the PDPA provides for restrictions on transferring personal data overseas; and penalties under the PDPA, which include remedial directions and financial penalties.

Chapter 3 of the Advisory Guidelines on the PDPA for selected topics, published by the PDPC and revised on 11 September 2014, provides guidance on the techniques, challenges and limitations in the anonymisation of personal data.

UNITED KINGDOM

ICO publishes updated IT security guide for small businesses

On 6 January 2016, the Information Commissioner's Office (***ICO***) published a revised guide to IT security (***Guide***) aimed at assisting and equipping small businesses (***Businesses***) with practical knowledge on implementing appropriate and effective IT security systems. First published in 2012, the Guide sets out steps to enable Businesses to fulfil the obligation under the Data Protection Act 1998 to protect personal data that is collected. In particular, Businesses are required to implement appropriate security measures to prevent any accidental or deliberate data breach.

The following paragraphs provide a brief and non-exhaustive summary of the 10 practical steps set out in the Guide:

(a) **Assess the threats and risks to a Business.** A Business may review the personal data that it holds to determine the nature of how valuable, sensitive or confidential the personal data is; assess the risks to these data; and consider all processes that require the Business to collect, store, use and dispose personal data.

(b) **Get in line with Cyber Essentials.** The United Kingdom Government's Cyber Essentials Scheme recommends the following five key controls to keep personal data secure: (i) boundary firewalls and internet gateways; (ii) secure configuration; (iii) access control; (iv) patch management and software updates; and (v) malware protection.

(c) **Secure data on the move and in the office.** Businesses may increase the security of personal data by using good access control systems; encryption; remote disable or wipe facilities; and physically lock up back-up devices, CDs and USBs.

(d) **Secure data in the cloud.** Measures under this heading include the assessment of the cloud provider's security arrangements for the processing of personal data in its systems and the use of the two factor authentication for remote access to the personal data in the cloud.

(e) **Back up data.** Businesses may implement robust data backup strategies, preferably having at least one backup off-site, to protect against ransomware and unforeseen circumstances such as theft; and natural disasters such as floods and fires.

(f) **Train the employees.** Businesses may educate their employees on the potential security threats to personal data, for example phishing emails and malware; cultivate a security awareness culture; and keep abreast with developments of potential threats that are relevant to the Business.

(g) **Keep an eye out for problems.** Measures under this heading include: (i) regular checks on security software messages, access control logs and other reporting systems; (ii) regular vulnerability scans; and (iii) regular penetrations tests.

(h) **Know what a Business should be doing.** Measures under this heading include: (i) implementing a good personal data protection policy; (ii) ensuring compliance with legal requirements and industry guidance; (iii) and making available the relevant training materials concerning the data protection responsibilities of employees.

(i) **Minimise data.** Businesses may consider transferring archive personal data to a more secure location; and utilise specialist software or get additional assistance should

Businesses need to securely destroy personal data.

(j) **Ensure IT contractors know what they should be doing.** Businesses may ask for a security audit of the systems containing the personal data that the Businesses have provided to the IT contractor; review copies of security assessments of the IT contractor; check that contracts with the IT contractor are in writing and comply with the relevant data protection obligations; and ensure that the IT contractor conducts adequate and secure disposals of personal data.

In Singapore:

Section 24 of the PDPA requires organisations to protect personal data in their possession or under their control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks. The PDPA applies to information regardless of whether it is in electronic or in other forms.

*In the context of electronic personal data, the PDPC issued the Guide to Securing Personal Data in Electronic Medium (**PDPC Guide**) on 8 May 2015, which seeks to provide information and guidance on topics related to the security and protection of personal data stored in electronic medium. The PDPC Guide is especially relevant for individuals responsible for data protection within an organisation and individuals who supervise or work with ICT systems and processes.*

ICO consults on revised privacy notices code of practice

On 2 February 2016, the Information Commissioner's Office (***ICO***) launched a consultation on the revised "Privacy notices, transparency and control – a code of practice on communicating privacy information to individuals" (***Code***), which ends on 24 March 2016. The Code sets out measures to assist organisations to meet the requirements under the Data Protection Act 1998, in particular, the requirement to provide rights to individuals. Since it is challenging to utilise a single document to inform individuals of the choice and control that they have over how their personal data may be used, the revised Code seeks to develop a blended approach, by utilising a range of techniques, to communicate these rights to individuals.

The following paragraphs set out a brief and non-exhaustive summary of the key revisions to the Code:

(a) **Understanding individuals' reasonable expectations**. Organisations may consider undertaking privacy impact assessments; reviewing the implementation of previous similar personal data processing activities; utilising online questionnaires or focus groups to undertake research to gauge whether the wider public's reasonable expectations are in line with the organisations' plans to utilise personal data; and observing industry practice to find an effective approach to obtain a more informed picture about the reasonable expectations of individuals. If an individual's reasonable expectations differ from how an organisation plans to utilise the personal data, it will be appropriate for organisations to consider communicating privacy notices actively.

(b) **The Internet of Things**. Often, several separate data controllers will be involved in processing personal data in smart devices and each data controller have obligations to provide privacy notices as to how the personal data of individuals may be utilised.

(c) **Plan privacy notices.** Taking into consideration the current digital landscape, organisations may consider, amongst other things, how notices may be embedded into the organisation's processes and interactions with customers.

(d) **User testing**. Organisations may conduct user testing to receive feedback on a draft privacy notice, which may enable organisations to improve the privacy notice in terms of the usefulness and level of engagement with individuals.

(e) **Just-in-time notices, icons and symbols**. Just-in-time notices, icons and symbols are tools to effectively provide privacy notices. The former refers to notices which appear on the individual's screen at the point where the individual inputs personal data, providing a brief message explaining how the information that the individual is about to provide may be used while the latter refers to indicators that serve as useful reminders to the individual that data processing is taking place.

(f) **Privacy notices on mobile devices and smaller screens**. To ensure privacy notices on portable devices such as mobile devices and tablets are as readable as that reflected on a computer screen, organisations may use videos or just-in-time notices, which are particularly suitable for smaller devices, to communicate privacy notices.

In Singapore:

Generally, there is no specific requirement under the PDPA that compels organisations that hold the personal data of individuals to offer individuals the right to have a degree of choice or control over the use of their personal data. However, pursuant to section 16 of the PDPA, individuals have a right to withdraw consent given to an organisation in respect of the collection, use or disclosure by that organisation of personal data about the individual for any purpose. To facilitate organisations in meeting the obligation under this provision, the PDPC published a Guide on Sample Clauses for Obtaining and Withdrawing Consent on 8 May 2015 which sets out sample clauses for obtaining an individual's consent to collect, use or disclose his personal data for particular purposes, as well as for an individual to withdraw consent or otherwise indicate that the individual does not consent to the collection, use and disclosure of personal data.

An organisation may refer to the Guide to Notification issued by the PDPC on 11 September 2014, for information and examples of good practices when providing notification on an organisation's personal data policies and practices.

EUROPE

EU data protection reform

On 15 December 2015, the European Commission (***EC***), the European Parliament and the Council of the European Union reached an agreement to pass the EU Data Protection Reform (***Reform***), which was put forward by the EC in January 2012 to make Europe fit for the digital age.

This Reform, which consists of two instruments, is to be formally adopted in early 2016. The new rules will become applicable two years thereafter.

The first instrument is the General Data Protection Regulation (***Regulation***), which is aimed at enabling citizens in the EU to have better control of their data, and in addition, allowing businesses to make the most of opportunities in the Digital Single Market by cutting red tape and benefiting from reinforced consumer trust.

The second instrument, aimed at the police and criminal justice sector, is the Police and Judicial Co-operation Data Protection Directive. The objective of this Directive is to facilitate an increase in cross-border cooperation and sharing of information across Member States, and to ensure that the data of individuals involved in criminal proceedings receive appropriate protection.

The new rules under the Regulation seek to strengthen the existing rights of and empower individuals with more control over their personal data, including:

(a) **Easier access to individuals' data**: individuals will have more information on how their data is processed and such information can be made available in a clear and understandable manner;

(b) **A right to data portability**: it will be easier for individuals to transfer personal data between service providers;

(c) **A clarified "right to be forgotten"**: when an individual no longer wants his or her data to be processed and, provided that there are no legitimate grounds for retaining it, the data will be deleted;

(d) **The right to know when personal data has been hacked:** for example, organisations are required to notify the national supervisory authority of serious data breaches as soon as possible so that users can take appropriate measures.

The Regulation also seeks to further unify Europe's rules on data protection, in order to establish clear and modern rules for businesses, so as to create business opportunities for organisations and encourage innovation in today's digital economy. Amongst other things, the Regulation will:

(a) Establish one single set of rules which will make it simpler and cheaper for companies to do business in the EU.

(b) Provide a one-stop-shop for businesses, which will only have to deal with one single supervisory authority. This is estimated to save €2.3bn (S$3.5bn) per year.

(c) Apply the same rules to companies based outside of Europe when offering services in the EU.

(d) Avoid a burdensome one-size-fits-all obligation and rather tailor them to the respective risks.

(e) Guarantee that data protection safeguards are built into products and services from the earliest stage of development (Data protection by design). Privacy-friendly techniques such as pseudonomysation will be encouraged, to reap the benefits of big data innovation while protecting privacy.

In addition, the Regulation seeks to stimulate economic growth by cutting costs and red tape for European business, especially for small and medium enterprises (SMEs). SMEs will benefit from:

(a) Scrapping of notifications to supervisory authorities, thereby reducing costs incurred by businesses of €130m (S$200m) every year.

(b) Granting SMEs the ability to charge a fee for providing access, where requests to access data are manifestly unfounded or excessive.

(c) Exempting SMEs from the obligation to appoint a data protection officer insofar as data processing is not their core business activity.

(d) Exempting SMEs from the obligation to carry out an impact assessment unless there is a high risk.

With the new Data Protection Directive for Police and Criminal Justice Authorities, law enforcement authorities in EU Member States will be able to more efficiently and effectively cooperate and exchange information necessary for investigations, with a view to preventing and/or taking enforcement action against crime and terrorism in Europe. All law enforcement processing must however comply with the principles of necessity, proportionality and legality, with appropriate safeguards for the individuals. Supervision must be carried out by independent national data protection authorities, and effective judicial remedies are to be provided for.

Further, the Data Protection Directive for Police and Criminal Justice Authorities provides clear rules for the transfer of personal data by law enforcement authorities *outside* the EU, to ensure that the level of protection of individuals guaranteed in the EU is not undermined.

In Singapore:

*The PDPA, which came into full force on 2 July 2014, establishes a general data protection framework which governs the collection, use and disclosure of individuals' personal data by organisations in the private sector. There are nine key data protection obligations, as well as the Do Not Call (**DNC**) obligations under the data protection framework in the PDPA. The PDPC has also issued a variety of guidelines, ranging from main advisory guidelines to sector-specific advisory guidelines. The Guide to Securing Personal Data in Electronic Medium and the Guide to Managing Data Breaches, both published on 8 May 2015, are recent guidelines that are especially relevant for the digital age.*

On 10 March 2015, the Minister for Communications and Information commented in Parliament that as aspects of individuals' lives, identities and personae become deeply intertwined with the technology that pervades their lives, protecting personal data becomes ever more critical. In this regard, the Singapore Government has taken the first step, with the introduction of the PDPA in 2012. Through consultations with the public, private and people sectors, a framework of regulations and guidelines that balances the interests of consumers and businesses was formulated. The PDPC continues to work closely with stakeholders through public consultations. It has continually sought industry's input for advisory guidelines that establish sectoral norms on personal data protection, and for specific areas of interest. The PDPC will continue to develop additional guidelines with public feedback.

ECHR held that Romanian courts had struck fair balance between employee's right to private life and employer's interests in the context of employer's monitoring of employee's instant messaging communications at workplace

In a case concerning an employer's monitoring of an employee's instant messaging communications at the workplace, the European Court of Human Rights (***ECHR***) held that there was nothing to indicate that the Romanian courts had failed to strike a fair balance between an employee's right to respect for his private life under Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms (***Convention***)[1] and his employer's interests.

Background

Mr Bodgan Mihai Bărbulescu (***Employee***), a Romanian national, was requested by his employer to create a Yahoo Messenger account for the purpose of responding to clients' queries. His Yahoo messenger communications were monitored by his employer over a period of nine days, and the records showed that he had used the Internet and Yahoo Messenger for personal purposes, in breach of his employer's internal regulations, which stated that: "*[i]t is strictly forbidden to disturb order and discipline within the company's premises and especially … to use computers, photocopiers, telephones, telex and fax machines for personal purposes.*" His employment was terminated for breach of these internal regulations.

The Romanian Court of Appeal (which upheld the County Court's judgement) held that the employer's conduct had been reasonable, and that the monitoring of the Employee's communications had been the only method of establishing if there had been a disciplinary breach.

The Employee then lodged an application with the European Court of Human Rights, alleging that his employer's decision to terminate his contract had been based on a breach of his right to respect for his private life and correspondence, and that the domestic courts had failed to protect his right.

The ECHR Decision

The ECHR had to examine whether the Employee had a reasonable expectation of privacy when communicating from the Yahoo messenger account that he had registered at his employer's request. In this regard, the ECHR noted that it was not disputed that the employer's internal regulations strictly prohibited employees from using the company's computers and resources for personal purposes. The ECHR therefore had to determine whether in view of the general prohibition imposed by the employer, the Employee retained a reasonable expectation that his communications would not be monitored.

Applicability of Article 8 of the Convention

The ECHR held that Article 8 of the Convention was applicable. Some factors considered by the ECHR in coming to that decision were that:

(a) the employer accessed the Employee's Yahoo messenger account (including his personal account);

(b) the transcript of the Employee's communications was used as a piece of evidence in the domestic labour court proceedings; and

(c) the Government did not explicitly dispute that the content of the Employee's communications with his fiancée and brother was purely private.

Merits of the Employee's application

The ECHR noted that although the purpose of Article 8 of the Convention is essentially to protect an individual against arbitrary interference by public authorities, it does not merely compel the State to abstain from such interference: in addition to this primarily negative undertaking, there may be positive obligations inherent in an effective respect for private life, such as the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals between themselves. In both contexts, regard must be had to the fair balance that has to be struck between competing interests, which may include competing private and public interests or Convention rights, and in both contexts, the State enjoys a certain margin of appreciation.

[1] Article 8 of the Convention provides that:

> "*1. Everyone has the right to respect for his private and family life, his home and his correspondence.*
> *2. There shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*"

Therefore, the ECHR had to examine whether the State, in the context of its positive obligations under Article 8 of the Convention, had struck a fair balance between the applicant's right to respect for his private life and correspondence. In this regard, the ECHR noted that the scope of the complaint was limited to the monitoring of the Employee's communications within the framework of disciplinary proceedings.

The ECHR concluded that there was nothing to indicate that the domestic authorities failed to strike a fair balance, within their margin of appreciation, between the Employee's right to respect for his private life under Article 18 and his employer's interests. In this regard, the ECHR found that it was not unreasonable for an employer to take steps to verify that employees are completing their professional tasks during working hours. In addition, the ECHR found that the employer's monitoring was limited in scope and proportionate, as it appeared that the communications on the Employee's Yahoo Messenger account was examined, but not the other data and documents that were stored on his computer. Further, the ECHR also found that the applicant had not convincingly explained why he had used his Yahoo messenger account for personal purposes. Accordingly, the ECHR found that there has accordingly been no violation of Article 8 of the Convention.

<u>*Partly dissenting opinion*</u>

The dissenting opinion noted that the novel features of the case concerned the non-existence of an Internet surveillance policy, the personal and sensitive nature of the Employee's communications that were accessed by the employer, and the wide scope of disclosure of these communications during the disciplinary proceedings brought against the Employee.

The dissenting judge observed that new technologies make prying into the Employee's private life both easier for the employer and harder for the Employee to detect, the risk being aggravated by the connatural inequality of the employment relationship. A human-rights centred approach to internet usage in the workplace warrants a transparent internal regulatory framework, a consistent implementation policy and a proportionate enforcement strategy by employers. The judge noted that such a regulatory framework, policy and strategy were totally absent in the present case.

In this regard, the judge opined that the interference with the applicant's right to privacy was the result of a dismissal decision taken on the basis of an *ad hoc* Internet surveillance measure by the applicant's employer, with drastic spill over effects on the applicant's social life. The domestic courts confirmed the Employee's disciplinary punishment, on the basis of the same evidence gathered by the surveillance measure. In the judge's view, the clear impression arising from the file was that the local courts willingly condoned the employer's seizure upon the Internet abuse as an opportunistic justification of removal of an unwanted employee whom the company was unable to dismiss by lawful means. The judge concluded that although the domestic courts could have remedied the violation of the Employee's right to respect for private life, they opted to confirm that violation. The ECHR did not provide the necessary relief either, and for that reason, the judge dissented.

In Singapore:

*Under the PDPA, organisations may collect personal data from their employees without consent as long as the collection is reasonable for the purposes of managing or terminating the employment relationship.[2] The non-legally binding Advisory Guidelines on the Personal Data Protection Act for Selected Topics (**Advisory Guidelines**) issued by the PDPC state that such purposes could include, amongst other things, monitoring how the employee uses company computer network resources. The consent of employees would not be required if the use[3] or disclosure[4] of such personal data is consistent with the purpose of that collection.*

While consent is not required, section 20(4) of the PDPA provides that organisations are required to notify their employees of: (a) the purposes of such collection, use and disclosure; and (b) on request by the employee, the business contact information of a person who is able to answer the employee's questions about that collection, use or disclosure on behalf of the organisation, on or before organisations collect, use or disclose personal data of an individual for purposes of managing or terminating an employment relationship.

[2] Paragraph 1(o) of the Second Schedule of the PDPA.

[3] Paragraph 1(j) of the Third Schedule of the PDPA.

[4] Paragraph 1(s) of the Fourth Schedule of the PDPA.

Therefore, in the Singapore context, it appears that while employers may collect personal data of employees without consent for the purpose of monitoring how employees use company computer network resources, employers are required to notify their employees of the purposes of the collection, use or disclosure of personal data, and provide the business contact information of the relevant person who can answer the employee's questions about such collection, use or disclosure of personal data.

Court of Justice of the European Union declares European Commission's US Safe Harbour decision invalid

On 6 October 2015, in the case of *Maximillian Schrems v Data Protection Commissioner (Case C-362/14)* (***ECJ Decision***), the Court of Justice of the European Union (***ECJ***) declared that the decision of the European Commission (***Commission***) dated 26 July 2000 that under the "safe harbour" scheme, the United States ensures an adequate level of protection of personal data transferred (***Safe Harbour Decision***), was invalid.

The ECJ also held that the existence of a Commission decision finding that a third country ensures an adequate level of protection of the personal data transferred cannot eliminate or even reduce the powers available to national supervisory authorities under the Charter of Fundamental Rights of the European Union and Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (***Data Protection Directive***).

Background to the original Safe Harbour framework

The Data Protection Directive provides that the transfer of personal data from a European Union (***EU***) Member State to a third country may, in principle, take place only if the third country in question ensures an adequate level of protection of the data. The Data Protection Directive also provides that the Commission may find that a third country ensures an adequate level of protection by reason of its domestic law or its international commitments. Further, the Data Protection Directive provides that each Member State is to designate one or more public authorities responsible for monitoring the application within its territory of the national provisions adopted on the basis of the Data Protection Directive.

The Safe Harbour framework (***Framework***) comprised a set of Safe Harbour Privacy Principles (***Principles***) and accompanying Frequently Asked Questions (***FAQs***) issued by the United States Department of Commerce. Pursuant to Commission Decision 2000/520/EC of 26 July 2000, the Commission recognised that for the purposes of the Data Protection Directive, the Framework is considered to ensure an adequate level of protection for the transfer of personal data from the EU to organisations established in the United States who have self-certified their adherence to the Principles implemented in accordance with the FAQs.

The ECJ Decision

The ECJ Decision concerned one Maximillian Schrems, an Austrian citizen and Facebook user. As is the case with other Facebook users residing in the EU, some or all of the data provided by Mr. Schrems was transferred from Facebook's Irish subsidiary to servers located in the United States, where it is processed.

Mr. Schrems lodged a complaint with the Irish supervisory authority, the Data Protection Commissioner (***DPC***), taking the view that in light of Edward Snowden's revelations concerning the activities of United States intelligence services (such as the National Security Agency), the law and practice of the United States do not offer sufficient protection against surveillance by public authorities of data transferred to that country. The DPC rejected Mr. Schrem's complaint on the ground, in particular, that in the Safe Harbour Decision, the Commission had considered that under the Framework, the United States ensured an adequate level of protection of the personal data transferred.

Mr. Schrems then brought an action before the High Court of Ireland challenging the decision in the main proceedings, and the High Court referred the case to the ECJ, which held that:

(a) the existence of a Commission decision finding that a third country ensures an adequate level of protection of the personal data transferred cannot eliminate or even reduce the powers available to national supervisory authorities under the Data Protection Directive; and

(b) the Safe Harbour Decision was invalid.

The powers of national data protection authorities

The ECJ held that the existence of a Commission decision finding that a country ensures an adequate level of protection of the personal data transferred cannot eliminate or reduce the powers available to national supervisory authorities. In this regard, the ECJ noted that no provision of the Data Protection Directive prevents oversight by national supervisory authorities of transfers of personal data to third countries which have been the subject of a Commission decision. Therefore, even if the Commission has adopted a decision, the national supervisory authorities, when dealing with a claim, must be able to examine, with complete independence, whether the transfer of a person's data to a third country complies with the requirements laid down by the Data Protection Directive. Ultimately, the ECJ has the task of determining the validity of a Commission decision.

The validity of the Safe Harbour Decision

The ECJ found that the Safe Harbour Decision was invalid.

At the outset, the ECJ noted that the Commission was required to find that the United States ensures, by reason of its domestic law or its international commitments, a level of protection of fundamental rights essentially equivalent to that guaranteed within the EU under the Data Protection Directive. The ECJ observed that the Commission did not make this finding. Further, the ECJ observed that the Framework is applicable solely to United States undertakings which adhere to the Framework, and that the United States public authorities are not subject to the Framework. In addition, national security, public interest and law enforcement requirements of the United States prevail over the Framework, which therefore enables interference by United States public authorities with the fundamental rights of persons.

Importantly, the ECJ stated that protection of the fundamental right to respect for private life at the EU level requires derogations and limitations in relation to the protection of personal data to apply only insofar as strictly necessary. In this case, the ECJ found that legislation is not limited to what is strictly necessary where it authorises, on a generalised basis, storage of all the personal data of all the persons whose data is transferred from the EU to the United States without any differentiation, limitation or exception being made in light of the objective pursued, and without an objective criterion being laid down for determining the limits of access of the public authorities to the data and of its subsequent use. The ECJ added that legislation permitting public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life. The ECJ also observed that legislation which does not provide for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, compromises the essence of the fundamental right to effective judicial protection.

The ECJ also found that the Safe Harbour Decision denies the national supervisory authorities their powers where a person calls into question whether the Safe Harbour Decision is compatible with the protection of privacy and of the fundamental rights and freedoms of individuals. In this regard, the ECJ held that the Commission did not have the competence to restrict the national supervisory authorities' powers in that way.

For these reasons, the ECJ declared the Safe Harbour Decision invalid. In this connection, the DPC will be required to examine Mr. Schrem's complaint with all due diligence and at the conclusion of its investigation, to decide whether pursuant to the Data Protection Directive, transfer of the data of Facebook's European users to the United States should be suspended on the ground that the United States does not afford an adequate level of protection of personal data.

Privacy Shield

On 2 February 2016, the Commission announced that the Commission and the United States have agreed on a new framework for transatlantic data flows – the EU-US Privacy Shield (***Privacy Shield***). This new framework is intended to protect the fundamental rights of Europeans where their data is transferred to the United States and ensure legal certainty for businesses.

According to the Commission, the Privacy Shield reflects the requirements set out by the ECJ in the ECJ Decision, which declared the old Framework invalid. The new Privacy Shield is intended to provide stronger obligations on companies in the

United States to protect the personal data of Europeans and stronger monitoring and enforcement by the United States Department of Commerce and Federal Trade Commission, including through increased co-operation with European data protection authorities. Further, the Privacy Shield includes commitments by the United States that possible access by public authorities to personal data transferred under the new framework would be subject to clear conditions, limitations and oversight, preventing generalised access. Europeans will also be able to raise any enquiry or complaint in this context with a dedicated new Ombudsperson.

The new Privacy Shield arrangement is expected to include the following elements:

(a) **Stronger obligations on companies handling Europeans' personal data and robust enforcement**
- In general, the new arrangement will be transparent and contain effective supervision mechanisms to ensure that companies respect their obligations, including sanctions or exclusion if they do not comply.
- The new rules also include tightened conditions for onward transfers to other partners by the companies participating in the scheme.
- United States companies wishing to import personal data from Europe need to commit to robust obligations as regards how personal data is processed and how individual rights are guaranteed.
- The Department of Commerce will monitor that companies publish their commitments, which makes them enforceable under United States law by the United States Federal Trade Commission.
- Any company handling human resources data from Europe has to commit to comply with decisions by European data protection authorities.

(b) **Clear safeguards and transparency obligations on United States government access**
- The United States has given the EU written assurances that access by public authorities for law enforcement and national security will be subject to clear limitations, safeguards and oversight mechanisms, and these exceptions must be used only to the extent necessary and proportionate.
- The United States has ruled out indiscriminate mass surveillance on the personal data transferred to the United States under the new arrangement.
- There will be an annual joint review by the Commission and the United States Department of Commerce to regularly monitor the functioning of the arrangement, which will also include the issue of national security access.

(c) **Effective protection of EU citizens' rights with several redress possibilities**
- Companies will have deadlines to reply to complaints.
- European data protection authorities may refer complaints to the United States Department of Commerce and the Federal Trade Commission.
- Alternative dispute resolution will be free of charge.
- For complaints on possible access by national intelligence authorities, a new Ombudsperson will be created.

On 29 February 2016, the Commission issued legal texts that will put in place the Privacy Shield, as well as a communication summarising actions taken in the past years to restore trust in transatlantic data flows since the 2013 surveillance revelations. The documents include a draft "adequacy decision" of the Commission, the texts which will constitute the Privacy Shield, the Privacy Shield Principles which companies have to abide by, as well as written commitments by the United States Government (to be published in the United States Federal Register) on the enforcement of the arrangement, including assurance on the safeguards and limitations concerning access to data by the public authorities. Once adopted, the Commission's adequacy finding establishes that the safeguards provided when data is transferred under the new Privacy Shield are equivalent to data protection standards in the EU.

In Singapore:

Pursuant to section 26 of the PDPA, organisations must not transfer any personal data to a country or territory outside Singapore except in accordance with requirements prescribed under the PDPA to ensure that organisations provide a standard of protection to personal data so transferred that is comparable to the protection under the PDPA. An

organisation may transfer personal data outside Singapore if it has taken appropriate steps to ensure that it will comply with the data protection provisions under the PDPA in respect of the transferred personal data while such personal data remains in its possession or under its control; and if the personal data is transferred to a recipient in a country or territory outside Singapore, that the recipient is bound by legally enforceable obligations to provide to the personal data transferred a standard of protection that is comparable to that under the PDPA.

AROUND THE WORLD

TPP provisions pertaining to the protection of personal information

On 4 February 2016, Singapore, together with Australia, Brunei Darussalam, Canada, Chile, Japan, Malaysia, Mexico, New Zealand, Peru, the United States, and Vietnam (***TPP Parties***) signed the Trans-Pacific Partnership agreement (***TPP Treaty***) in Auckland, New Zealand. In order for the TPP Treaty to take effect, it will need to be further ratified by each TPP Party within a period of two years from 4 February 2016.

The TPP Treaty, in particular, chapter 14 of the TPP Treaty entitled "Electronic Commerce", contains specific provisions pertaining to the protection of personal information. Personal information is defined as any information, including data about an identified or identifiable natural person.

Specifically, Article 14.8(2) requires each TPP Party to adopt or maintain a legal framework to provide protection of the personal information of users of electronic commerce. In addition, Article 14.8(5) encourages each TPP Party to develop mechanisms to promote the compatibility between the different data protection regimes of each TPP Party.

Notably, there are provisions that appear to facilitate the cross border flows of information by electronic means. For instance, Article 14.11(2) of the TPP Treaty requires each TPP Party to allow the cross-border transfer of information, including personal information, by electronic means when conducting the business of a covered person. For the purposes of this Article and Article 14.13(2) below, "business" is left undefined and a "covered person" is defined as:

(a) an investor of a TPP Party who has an investment in another TPP Party's territory;

(b) a citizen, permanent resident or an enterprise of a TPP Party that attempts to, is making, or has made an investment in the territory of another TPP Party (excluding an investor in a financial institution); or

(c) a service supplier of a TPP Party (i.e. a citizen, permanent resident or an enterprise who seeks to supply or supplies a service).

However, a covered person does not include:

(d) a citizen, permanent resident or an enterprise of a TPP Party that is engaged in the business of supplying a financial service within the territory of the TPP Party and that seeks to supply or supplies a financial service through the cross-border supply of such a service; and

(e) any financial intermediary or other enterprise that is authorised to do business and is regulated or supervised as a financial institution under the law of the TPP Party in whose territory it is located.

In addition, there are also provisions that appear to facilitate the use of computing facilities. Computing facilities are defined as computer servers and storage devices for processing or storing information for commercial use. For example, under Article 14.13(2) of the TPP Treaty, TPP Parties are prohibited from making it a condition, for a covered person conducting business in the TPP Party's territory, to use or locate computing facilities in that TPP Party's territory. This means that a covered person cannot be bound by any condition, when conducting business in a TPP Party's territory, to prevent the covered person from using or locating computing facilities outside the TPP Party's territory.

Furthermore, there are provisions that appear to facilitate the regulation of unsolicited commercial electronic messages. An unsolicited commercial electronic message is defined as an electronic message sent for commercial or marketing purposes to an electronic address, without the consent of the recipient or despite the explicit rejection of the recipient, through an Internet access service supplier or, to the extent provided for under the laws and regulations of each TPP Party, other telecommunications service. For instance, under Article 14.14 of the TPP Treaty,

each TPP Party is required to adopt or maintain measures regarding unsolicited commercial electronic messages that:

(a) require suppliers of unsolicited commercial electronic messages to facilitate the ability of recipients to prevent ongoing reception of those messages;

(b) require the consent, as specified according to the law and regulations of each party, of recipients to receive commercial electronic messages; or

(c) otherwise provide for the minimisation of unsolicited commercial electronic messages.

Lastly, there are provisions that appear to facilitate cross-border cooperation in relation to the regulation of electronic commerce. Under Article 14.15 of the TPP Treaty, TPP Parties are to endeavour to exchange information and share experiences on regulations, policies, enforcement and compliance regarding electronic commerce, including personal information protection.

In view of how recently the TPP Treaty was signed, the tangible impact of its Articles as summarised above remains to be seen. What we do know is that these Articles pertaining to the protection of personal information are tailored specifically towards the regulation of personal information in an electronic commerce landscape. That said, as its provisions do bear some similarity with the national data protection laws of various signatory countries, upon ratification by these signatory countries, it is likely that the TPP Treaty will seek to enhance the harmonisation of the data protection principles across multiple jurisdictions.

COMPARATIVE TABLE (OVERVIEW)

FOR ASEAN JURISDICTIONS WITH COMPREHENSIVE DATA PROTECTION LAWS

	Singapore	Malaysia	Philippines
Data protection law and authority	Personal Data Protection Act 2012, enforced by the Personal Data Protection Commission	Personal Data Protection Act 2010, enforced by the Personal Data Protection Commissioner	Data Privacy Act of 2012, to be enforced by the National Privacy Commission[5]
Concept of sensitive personal data	No	Yes	Yes, referred to as "sensitive personal information".
Registration with data protection authority	No	Yes, for data users (i.e. excludes data processors) within specified classes	No
Data protection officer	Yes	No	Yes
Exemptions to consent/notification requirements	Yes	Yes	Yes
Concept of data intermediary	Yes "organisation" v. "data intermediary"	Yes "data user" v. "data processor"	Yes "personal information controller" v. "personal information processor"
Right to withdraw consent	Yes	Yes	Not clear. No express provision on withdrawal of consent
Right to access/correct personal data	Yes	Yes	Yes
Data retention limits	Yes No longer than necessary for the fulfilment of purposes for which data was collected, and for legal or business purposes.	Yes No longer than necessary for the fulfilment of purposes for which data was collected.	Yes. No longer than necessary for the fulfilment of purposes for which data was collected; legitimate business purposes; and/or legal purposes

[5] Data protection authority has not yet been constituted.

	Singapore	Malaysia	Philippines
Security obligations	'reasonable security arrangements' to protect personal data from security risks.	'practical steps' to protect personal data, having regard to certain factors.	'reasonable and appropriate organisational, physical and technical measures', having regard to certain factors.
Restrictions on overseas transfers of personal data	Yes	Yes	Yes
Penalties	• Remedial directions (including financial penalties) • Monetary fines and/or imprisonment for certain offences	• Monetary fines and/or imprisonment • Rejection of registration renewal • Revocation of registration	Monetary fines and/or imprisonment
Private civil claims	Yes	Not clear. No express statutory provision, but mentioned in Parliamentary debates	Yes

The Drew & Napier Telecommunications, Media and Technology Team

For more information on the TMT Practice Group, please click **here**.

Lim Chong Kin • Director and Head of TMT Practice Group

Chong Kin practices corporate and commercial law with strong emphasis in the specialist areas of TMT law and competition law. He regularly advises on regulatory, licensing, competition and market access issues. Apart from his expertise in drafting "first-of-its-kind" competition legislation, Chong Kin also has broad experience in corporate and commercial transactions including mergers and acquisitions. He is widely regarded as a pioneer in competition practice in Singapore and the leading practitioner on TMT and regulatory work. Chong Kin has won plaudits *for* '*good knowledge of the telecommunications industry and consistently excellent service*' *(**Asia Pacific Legal 500**);* and is cited to be '*really exceptional - he has the pragmatism, he's plugged-in, and he gives solid, clear advice,*' *(**Chambers Asia 2016***: Standalone Band 1 for TMT*);* and has been endorsed for his excellence in regulatory work and competition matters: ***Practical Law Company's Which Lawyer Survey 2011/2012; Who's Who Legal: TMT 2016*** and the ***Who's Who Legal: Competition 2015***. ***Asialaw Profiles*** notes: "*He's provided excellent client service and demonstrated depth of knowledge. Always responsive and available for ad hoc assistance."*

Tel: +65 6531 4110 • Fax: +65 6535 4864 • Email: **chongkin.lim@drewnapier.com**

Charmian Aw • Director

Charmian is a Director in Drew & Napier's TMT Practice Group. She is frequently involved in advising companies on a wide range of corporate, commercial and regulatory issues in Singapore. Charmian has also been actively involved in assisting companies on Singapore data protection law compliance, including reviewing contractual agreements and policies, conducting trainings and audits, as well as advising on enforcement issues relating to security, access, monitoring, and data breaches. Charmian is "recommended for corporate-related TMT and data privacy work" by ***The Asia Pacific Legal 500 2016***, and a Leading Lawyer in ***Who's Who Legal TMT 2016***. In 2015, she was listed as one of 40 bright legal minds and influential lawyers under the age of 40 by **Asian Legal Business** and **Singapore Business Review** respectively.

Tel: +65 6531 2235 • Fax: +65 6535 4864 • Email: **charmian.aw@drewnapier.com**

Daniel Teo • Director

Daniel is a Director in Drew & Napier's TMT Practice Group. Daniel's main practice areas are in telecommunications, media and technology; data protection; and corporate law. He frequently advises the telecommunications regulator and companies, particularly those in the technology sector, on various corporate and regulatory issues in Singapore. Daniel also handles general corporate work, such as review and drafting of agreements, and advising companies on a range of corporate, commercial and regulatory issues in Singapore.

His commercial dispute resolution experience in shipping and other commercial matters also saw him representing local and foreign companies in litigation and arbitration proceedings.

Tel: +65 6531 2328 • Fax: +65 6535 4864 • Email: **daniel.teo@drewnapier.com**