Baker & McKenzie

Cybersecurity Counter-offensive

Asia Pacific Guide

Contents

AUSTRALIA	1
CHINA	6
HONG KONG	12
INDIA	18
INDONESIA	22
JAPAN	25
MALAYSIA	30
PHILIPPINES	35
SINGAPORE	40
SOUTH KOREA	44
TAIWAN	49
THAILAND	54
VIETNAM	58

Introduction

Your organisation has been the target of a cybersecurity attack.
Now what do you do? What can you do?

Worldwide governments and organisations are, in the face of increasing numbers of cybersecurity incidents, turning their focus to how to manage cybersecurity threats and deal with the aftermath of cybersecurity incidents. For many organisations, the most common cybersecurity threat is the risk of confidential information being accessed and potentially misused by an external and/or adverse party i.e. data breaches.

One of the key challenges in responding to data breaches is that data can be taken from one or more jurisdictions, and moved very quickly to other jurisdictions. The cross border nature of incidents can make investigating a data breach, identifying your various obligations in relation to the data breach and identifying your options for dealing with the data breach, a very complex and daunting process. This is especially so because speed is almost always a critical factor in an effective response.

In the Asia Pacific region, recent years have seen a wave of new cybersecurity legislation, government established bodies to regulate or monitor cybersecurity and guidelines/reports being issued by governments and regulators. For example, in 2015, Indonesia and Singapore each introduced cyber agencies, Japan enacted the Cyber Security Basic Act and the Australian Securities and Investments Commission released a report on cyber resilience. For a number of countries in Asia Pacific, laws or guidelines on these issues are being formulated for the first time. In addition, countries such as the United States, where the Department of Justice released in April 2015 its "Best Practices for Victim Response and Reporting of Cyber Incidents", are adding to already existing systems of cybersecurity regulation.

Despite the increased regulatory activity, there is, unfortunately, no unified approach to the regulation of cybersecurity or the potential legal remedies available in the context of data breaches in the Asia Pacific region. Depending on the jurisdiction, data breach incidents may involve, in addition to laws regarding cybersecurity, obligations under privacy laws, employment/labour laws, equitable rights and obligations, the law of equity, corporate governance, fiduciary duties and industry or sector specific regulations. In some jurisdictions, laws regarding state or national secrets may also be enlivened, especially when data is suspected to have been transferred out of the jurisdiction.

Accordingly, local knowledge of the obligations in each country and how each relevant regulator or court operates in practice is essential to navigating a response to a data breach incident and understanding which legal remedies may be available and which will be most effective. Using this knowledge, we are able to assist our clients to investigate data breaches, to identify reporting obligations, to discuss strategies to minimise further disclosure of the data and mitigation of loss or damage, and to identify, where available, legal remedies to recover the data or loss associated with the data breach.

In this Guide, we:

- set out, in the remainder of this chapter, an outline of the preliminary assessment we recommend should be undertaken by clients when confronted with a suspected data breach; and
- identify, in the remaining chapters, for 13 countries in the Asia Pacific region, the position in response to a number of common issues which arise in dealing with a data breach incident. As you will see, while some jurisdictions with similar juridical history have similar processes, the type and availability of legal remedies can vary greatly across the region. In order to provide the broadest coverage of key jurisdictions, in addition to input from eleven jurisdictions in which Baker & McKenzie has offices in the region, we have also been very ably assisted by Kim, Choi & Lim in Korea and J. Sagar & Associates in India.

Effective triaging: conducting a preliminary assessment and determining next steps

Our advice to clients when faced with a suspected data breach is to act as quickly as possible to perform a preliminary assessment or triage of the situation.

Determine the nature of the compromised data and severity of the breach

That preliminary assessment should include identifying the nature and level of sensitivity of that data in terms of:

What information does the data contain? Is the data purely internal or does it include information belonging or relating to third parties? Does the data include personal or financial information?

What are the risks involved? Does the disclosure of the data present any risks of:

- identity theft;
- financial loss;
- humiliation of the data subject;
- damage to reputation;
- loss of business opportunity;
- loss of confidentiality of information which was a trade secret; or
- to personal safety; and

What are the legal implications? Does the disclosure result in any criminal, regulatory or contractual implications? Is there an obligation to provide a notification of the breach?

The following guidelines provide further assistance in conducting an assessment of the severity of the data breach.

DATA BREACH ASSESSMENT GUIDELINES

By considering the list of questions in these guidelines, you should be able to analyse the severity of a data breach, the possible consequences of the breach and identify your potential next steps.

Issue	Higher severity	Lower severity
What was the source of the information?		
Was the subject information sourced from customers/ clients or other third parties?	Yes	No
Was the subject information created by the organisation and capable of being described as a trade secret or confidential?	Yes	No
Was the subject information created by the organisation but is not capable of being described as confidential or a trade secret?	N/A	Yes
Is the subject information held for or on behalf of a third party, including a government?	Yes	No

Issue	Higher severity	Lower severity
What information was lost?		
Does the subject information contain confidential information, personal information or information capable of being characterised as a state secret? If yes, answer remaining questions in this section.	Yes	No
Does the subject information contain any credit card, bank account, online account and/or password information capable of being used to cause immediate loss to the data subject?	Yes	No
Does the subject information contain any health information, biometric information, other form of sensitive information or record of private behaviours or practices?	Yes	No
Does the subject information include indicia used to authenticate customers and customer accounts?	Yes	No
Does the subject information contain any government identifiers or information which has been deemed by the government to be confidential?	Yes	No
Does the subject information contain personal attributes or identifiers that are permanent or persistent? I.e. the information lost cannot be reset by the data subject?	Yes	No
If the subject information contains a number of items, consider the consequences of the data set as a whole: for example are names and addresses associated with particular services, needs or attributes? Is the subject information in the form of a customer list?	Yes	No
How many files were affected?	More files	Fewer files
How many individuals were affected?	More individuals	Less individuals

Issue	Higher severity	Lower severity
What is the nature of the breach and the perpetrator(s)?		
Was the data accessed or downloaded from a secure system? If not, consider circumstances of data access.	Yes	No
Was the breach due to or caused by an error in systems or procedures?	Yes	No
Is the nature and extent of the breach understood or uncertain?	Uncertain	Understood
Do you know who caused the breach and the location of the data?	No	Yes
What does the breach suggest about the party that has obtained the information? Are they: – hacktivist? – organised crime? – competitor? – business opportunist including current or former employee or contractor or current or former party who had been given access to systems? – accidental recipient?	Hacktivist, organised crime, competitor	Business opportunist, accidental recipient
Has the breach resulted in or is it likely to result in publication of the information?	Yes	No
Has the breach resulted in or is it likely to result in the use of the information for criminal or financial gain?	Yes	No
Is it possible that the information is held by one person or does it appear likely that it has been sold or distributed?	Sold or distributed	Held by one person
When did the breach/s first occur?	Recently	Some time ago
Did the breach involve repeated unauthorised access? If so, how long have they been going on?	Longer period of time	Shorter period of time
Is the breach the same or similar to one that has been suffered previously and come to public attention?	Yes	No

Issue	Higher severity	Lower severity
Does the breach indicate a failure to take reasonable steps to protect the information or a breach of any previous undertaking given in relation to the management of data?	Yes	No
What is the risk of harm to individual(s)?		
Are any affected individual(s) particularly vulnerable in the context of this breach? For example does the lost data contain address information for individuals whose location is confidential?	Yes	No
Is there a risk to one or more data subjects of identity theft or fraud?	High risk	Low risk
Is there a risk to one or more data subjects of financial loss?	High risk	Low risk
Is there a risk to the physical safety one or more data subjects?	High risk	Low risk
Is there a risk to the emotional wellbeing of one or more data subjects?	High risk	Low risk
Is there a risk of loss of business or employment opportunities or one or more data subjects?	High risk	Low risk
Is there a risk of humiliation, damage to reputation or relationships to one or more data subject?	High risk	Low risk
Is there a risk of workplace or social bullying or marginalisation to one or more data subjects?	High risk	Low risk
What is the risk of harm to your organisation?		
Is there a risk of the organisation losing business? For example, customers or government departments choosing not to utilise services in the future.	High risk	Low risk
Is there a risk of the organisation suffering financial loss?	Risk dependent on nature of data and volume accessed	Risk dependent on nature of data and volume accessed

Issue	Higher severity	Lower severity
Is there a risk of the organisation suffering reputational damage?	High risk if notification required	Low risk if no notification required
Is there a risk of the organisation incurring regulatory or criminal sanction?	High risk dependent on nature of information accessed and cause of breach	Low risk dependent on nature of information accessed and cause of breach
Is there a risk of further data breaches due to systems being comprised?	Yes	No
Has all of the subject information been retrieved?	No	Yes
Can the risk of identity theft be reduced or eliminated by changes to its system or advice to the affected individual or services?	No	Yes
Can the organisation remediate the breach, e.g. by compensating the individual(s)?	No	Yes
Is it possible to: – take all steps necessary to remediate any system failures; – prevent or compensate any harm; and – keep the data breach confidential?	No	Yes
If the matter cannot be kept secret, when is it likely to become public knowledge?	Sooner	Later
Is it possible for the organisation to be compensated for any loss of business or for any financial loss?	No	Yes
Is it possible to negotiate with regulatory or law enforcement officials in relation to any applicable sanctions?	No	Yes

Issue	Higher severity	Lower severity
Is there an obligation to notify of the breach?		
Is there an obligation to notify law enforcement of the data breach?	Yes	No
Is there an obligation to notify any regulatory or industry body of the data breach?	Yes	No
Is there an obligation to notify the data subject of the data breach or a person or organisation affected by the data breach?	Yes	No
Is there a contractual obligation to notify a party of a data breach?	Yes	No
Jurisdictional/law enforcement issues		
Was the breach cross-jurisdictional?	Yes	No
Did the breach involve more than one jurisdiction outside your home jurisdiction?	Yes	No
If the breach is cross jurisdictional, is there a reliable and timely legal system in the jurisdiction where we believe the data or persons responsible are located?	No	Yes
Can the subject information be retrieved, including through law enforcement or court involvement?	No	Yes
If it is possible to recover the information, how long will it take?	Long period	Short period

Determine where the information is now and what can you can do in that jurisdiction

As can be seen above, one of the indicators of a severe data breach is when the compromised data is suspected to have left the home jurisdiction.

Determining whether that has occurred will usually involve cybersecurity professionals using whatever means are at their disposal and appropriate in the circumstances to try to, in the first place, identify the details of the device used to access the relevant systems (the "primary hacking device").

In many cases the location of the primary hacking device is: (a) determined to be in a particular foreign jurisdiction; or (b) not possible to be immediately identified due to the use by the perpetrator of a cloud provider (also located in a foreign jurisdiction) as an intermediary.

If, due to the severity of the breach, further action needs to be taken at that stage to continue to trace the data through to the perpetrator of the breach (including through an innocent cloud computing provider), a number of important questions arise as to the legal processes and procedures available in that jurisdiction.

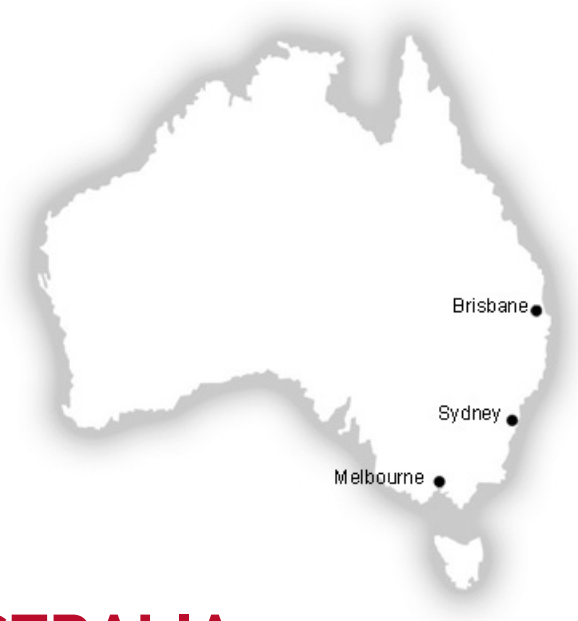
In particular, before taking further steps in a foreign jurisdiction, you should ask:

- Can further information be obtained if one of the way points is in another country or in an unknown location in the cloud?
- What type of legal action, if any, can be taken?
- Who has standing to take legal action?
- How easy or difficult is it to get relief needed?
- Are there any other legal issues to be aware of before commencing action?

The following chapters of this publication will assist you in answering those questions for 13 key jurisdictions in the Asia Pacific region. We hope you find them useful.

Co-editors

Patrick Fair and **Paul Forbes**



AUSTRALIA

Is it unlawful in this jurisdiction to access third party data without authorisation. Is it unlawful to store data which has been accessed without authority?

Yes.

There are a number of criminal offences under Federal and State laws in relation to the unauthorised access of data, which potentially carry prison sentences. The severity of the offence is largely related to the intention of the perpetrator on accessing and using the data. For example, if the data is accessed for the purposes of committing a further crime the punishment is more severe.

Persons who aid, abet, counsel, or procure someone to commit a criminal offence (which would likely include someone who stored data they knew to be improperly obtained or encouraged data to be improperly obtained) will also commit an offence. A person who assists the perpetrator after the data has been improperly obtained may also be guilty of an offence depending on the intention behind the accessing and use of the data by the original perpetrator.

The unauthorised access of data is not recognised as a traditional theft under Australian law.

In terms of civil actions, the unauthorised access of data may amount to a trespass. If the data accessed is confidential, there may also be claims available in contract (if there is a contractual obligation to keep the data confidential, which is common in many employment or business contracts) or in equity for breach of confidence (if the confidential information is improperly obtained or imparted in a manner which requires it not to be divulged). If a person is asked to store data which they know to have been obtained improperly, a claim may also be made against them for a breach of confidence.

Is there a legal mechanism whereby you can seek access to or retrieve the copy of data which has been accessed without authority? Is there a legal mechanism that enables you find out information about who may have accessed your data without authority and/or how it was used?

If you know who has taken the data or the identity of the person associated with the IP address of the device which accessed the data or where the data is being held there are options available to apply to access the copy of the data taken, find out information about who accessed the data and determine how the data may have been used.

If the identity of the person(s) who either committed the data breach or are storing or have stored the data at some point in time is known, the matter could be referred to the police or civil proceedings could be commenced to get access to information or documents. There are two civil processes which may be appropriate depending on the circumstances: preliminary discovery and/or search and seizure orders.

Preliminary discovery proceedings require an individual or company to produce documents so that either the identity of a potential defendant(s) can be determined or the plaintiff can assess whether there is a case to be made. Preliminary discovery may be sought where there is an issue about whether the access to data was authorised or whether the data was used to the detriment of its owner. If the only information known about the perpetrator of the data breach is the IP address associated with the breach, a preliminary discovery application could be made against the relevant Internet or cloud service provider to determine the identity of the account user.

Search orders are sought in the context of actual or anticipated civil proceedings. It is therefore necessary to know who is or are the intended defendant(s) to the civil proceedings. A search order requires the addressee to permit a team, comprised of the plaintiff's solicitor, an independent solicitor and where appropriate, an independent computer expert, to enter specific premises to search, inspect and either copy or remove documents (including storage drives or computers where

documents are stored electronically). Documents which are removed are not ordinarily provided to the plaintiff immediately but an order may be made for inspection by the plaintiff of those documents. In order to obtain a search order there must be a strong prima facie case against the defendant(s) and a real possibility that the defendant(s) may destroy or hide important evidentiary material.

If civil proceedings for breach of confidentiality obligations are brought and are ultimately successful, one of the orders made may be for the delivery up of the data accessed, damages or an account of profits.

Is there any restriction on the use that can be made of the information or documentation obtained regarding a data breach incident using a legal process?

Yes. In all Australian jurisdictions there is an express or implied obligation upon parties to only use documents produced in response to compulsory processes for the purposes of the proceeding in which they are produced. In relation to preliminary discovery proceedings, the information or documentation can be used to commence the proceedings anticipated.

It is possible to apply to the court under which jurisdiction the documents were produced to seek leave to use the information for the purposes of another proceeding and/or to disclose these documents to relevant law enforcement authorities.

Is it possible to maintain confidentiality in relation to the legal steps necessary to get access to the data or information?

Ordinarily no, but it is possible to ask the Court to make a suppression or non-publication order to keep the proceedings or their subject matter confidential. There is, however, a high threshold for meeting the requirements for the granting of a suppression order.

If it is later determined that proceedings should be commenced in another jurisdiction (for example, the perpetrator is found to reside there), can you stop the proceedings in this jurisdiction in such a way that you are not prevented from commencing proceedings on the same issue as a result of the application of res judicata, double jeopardy or some other similar principle?

Yes, if proceedings are stopped in a manner which does not result in a final determination of the issues in the proceeding. For example, withdrawing, discontinuing or staying the proceeding will usually not prevent a plaintiff from commencing proceedings either in this jurisdiction again or in another jurisdiction. However, there may be an issue if there is a final judgment or if the proceedings are "dismissed" or if

proceedings are actively on foot in two jurisdictions at the same time which cover the same issues.

As the description for the options for stopping proceedings may differ between Australian jurisdictions, it will be necessary to check the rules of the relevant court to determine the options for stopping the proceedings and the effect of utilising each option.

Is there an obligation in your jurisdiction to hold personal information securely?

Yes. Australian Privacy Principle 11 requires that certain regulated entities take such steps as are reasonable in the circumstances to protect personal information from misuse, interference and loss and from unauthorised access, modification and disclosure.

Does the law in your jurisdiction restrict or place conditions on the transfer of personal or other information to other foreign jurisdictions?

Yes. The Privacy Act 1988 requires that the transferring party must take such steps as are reasonable to ensure that the overseas recipient does not breach Australian Privacy Principles. In addition, unless certain disclosures are made and express consent obtained on the basis of the disclosures, the transferring party remains strictly liable for any data breach by the overseas recipient.

Is there a generally applicable obligation to notify data subjects of a data breach in your Jurisdiction?

No.

Is there a generally applicable obligation to notify the authorities of a data breach in your jurisdiction?

Possibly.

If the data breach was committed in the state of New South Wales and an individual knows or believes that it was done with the intention to commit a further crime and has information which that person believes might be of material assistance in securing the apprehension of the offender or their prosecution, that person may commit an offence if they do not, without reasonable excuse, bring the crime to the attention of the appropriate authorities. While the offence of failing to report is rarely prosecuted in practice it is something that should be considered.

The other Australian jurisdictions generally only make concealment of the data breach an offence if the concealment was in return for some gain. Again, while the bar for committing such an offence is quite high, this is a question that victims of a data breach should consider as part of dealing with a data security incident.

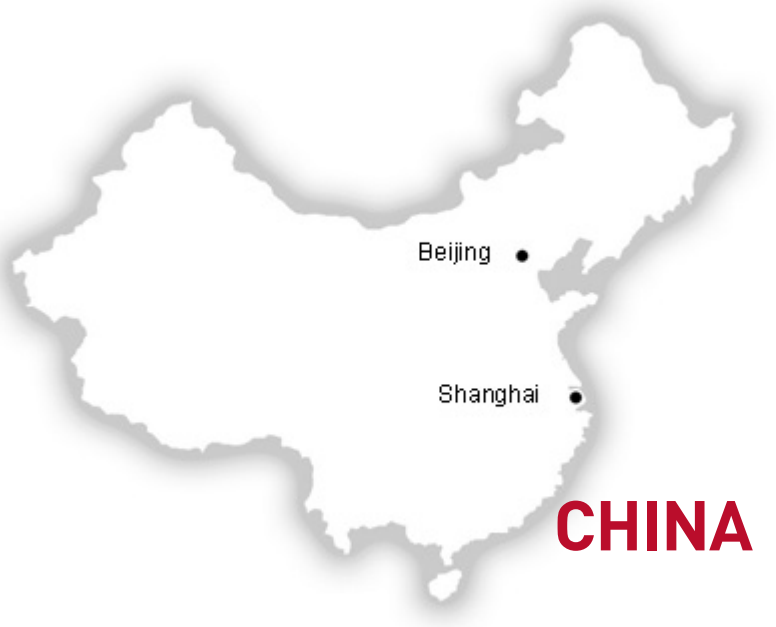
Are there sector specific mandatory data breach notification obligations in your jurisdiction?

Yes.

Prudential standards promulgated by the Australian Prudential Regulation Authority require notification of significant prudential breaches, including breaches associated with the integrity and security of data systems.

Patrick Fair
Partner, Sydney
+61 2 8922 5534
patrick.fair@bakerckenzie.com

Paul Forbes
Partner, Sydney
+61 2 8922 5346
paul.forbes@bakermckenzie.com



Is it unlawful in this jurisdiction to access third party data without authorisation? Is it unlawful to store data which has been accessed without authority?

The PRC Criminal Law broadly prohibits anyone from illegally obtaining personal data of others by stealing or any other means. If the circumstances are serious, the offender could be subject to imprisonment of up to three years and/or a fine. Where any entity commits such offence, it shall be fined, and the person in charge and other responsible personnel of the entity may also be subject to criminal penalties.

The *Decision of the Standing Committee of the National People's Congress on Strengthening the Protection of Network Information* also provides administrative penalties for stealing or otherwise illegally obtaining personal data of others, and selling or otherwise illegally providing personal data of others. These penalties include warnings, fines, confiscation of illegal gains, revocation of business license, closure of website, prohibition of the responsible personnel from engaging in internet services as well as being recorded on the social credit files and disclosed to the public.

In serious cases where the infringement on personal data constitutes acts against public security administration, the offender may be subject to penalties including warnings, fines and/or administrative detention of up to 20 days, according to the Law of the PRC on the Imposition of Penalties in connection with the Administration of Law and Order.

Please note that the laws mentioned above do not specify what constitutes "illegally obtaining" personal information. It is possible that under a broad interpretation, the term would cover unauthorised assess of data as well as storage of data depending on the intent of the offender.

In addition to criminal and administrative penalties, the PRC Tort Liability Law establishes a private right of action for infringement of one's right to privacy. The infringed party may seek compensation for actual losses (or profits arising from the infringement if actual losses cannot be determined) and where applicable, damages for emotional distress, in addition to other remedies provided under the law (e.g. cessation of infringement, return of property, apology from the infringer, restoration of reputation, etc.). Given the potentially broad scope of privacy rights, if a person accessed the personal data of others without authorisation or stored data which has been accessed without authorisation, such person may be subject to civil liabilities for infringement of the privacy rights of others.

Where the above infringement is committed by an internet user through the internet, the internet content service provider shall be jointly and severally liable with the internet user if (i) after being notified of the infringement, the internet content service provider fails to take necessary actions to remedy the infringement (such as deleting or blocking the infringing web content or disconnecting the link), which causes additional harm to the infringed party, or (ii) if the internet content service provider is aware that the internet user is committing the infringement through its internet services and fails to take necessary measures.

Is there a legal mechanism whereby you can seek access to or retrieve the copy of data which has been accessed without authority? Is there a legal mechanism that enables you find out information about who may have accessed your data without authority and/or how it was used?

Currently there is no specific legal mechanism to address or remedy a data breach. The infringed party may file a case against the data possessor or suspected infringer through an ordinary civil or criminal proceeding, and seek court assistance in collecting or preserving evidence (in a civil case) or rely on police investigations (in a criminal case).

However, the thresholds of initiating a criminal case could be high, and the costs of launching a civil lawsuit could be substantial, while the efficacy of these procedures to enable fact-finding by data subjects remains largely to be tested.

Is there any restriction on the use that can be made of the information or documentation obtained regarding a data breach incident using a legal process?

As mentioned above, currently there is no specific legal mechanism that aims to help data subjects to investigate and collect information regarding a data breach incident.

As a general comment, under the PRC Civil Procedure Law, the courts have the power to use "preservation measures" such as orders of specific performance or injunction, in situations where such measures are necessary to facilitate enforcement of judgment or prevent harm to be done to one party. Thus if the infringed party has brought a civil proceeding against the data possessor to retrieve and preserve relevant data records, it may also apply for a restrictive order requiring the data possessor to keep confidential any information or documentation thus obtained, to the extent necessary to prevent tip-off to the infringer and harm to the infringed party. However, as civil procedures involving data breach claims have been uncommon in China, it is unclear whether the courts would grant a restrictive order upon the application by the infringed party.

Under the PRC Criminal Procedure Law, evidence collected in a criminal proceeding shall be kept confidential if it concerns state secrets, trade secrets or personal information. Relevant entities and persons that are requested to cooperate with the police's technical investigation measures shall keep their involvement and relevant information confidential.

Is it possible to maintain confidentiality in relation to the legal steps necessary to get access to the data or information?

In a criminal proceeding, the pre-trial investigation phase should normally be quiet and secretive. At the trial stage, however, both civil and criminal cases shall be tried publicly, except for cases that involve state secrets, trade secrets or the private affairs of individuals. It remains to be tested if a case involving data breach incidents should be regarded as a case that involves privacy of individuals and thus be exempt from a public trial. In any event, courts are required to publicly pronounce their judgments regardless of whether the cases were tried publicly or not.

If it is later determined that proceedings should be commenced in another jurisdiction (for example, the perpetrator is found to reside there), can you stop the proceedings in this jurisdiction in such a way that you are not prevented from commencing proceedings on the same issue

as a result of the application of res judicata, double jeopardy or some other similar principle?

Yes, if the proceeding is stopped before a judgment or ruling is pronounced by the court.

The plaintiff in a civil action may apply for withdrawal of the case anytime before a judgment or ruling is pronounced and if the court decides to grant the approval, the plaintiff may commence proceeding on the same issue in this or another jurisdiction again, as long as the statutes of limitations permit.

Is there an obligation in your jurisdiction to hold personal information securely?

China does not have a comprehensive data privacy law that imposes general obligations to maintain personal information securely. However, various sector specific regulations impose security and confidentiality requirements on certain entities and individuals with access to personal information, for example:

- Telecommunications regulatory agencies, telecommunications business operators and internet information service providers and their personnel with respect to internet user information;
- Business operators and their personnel with respect to consumer information;
- Medical personnel, hospitals and public health authorities with respect to patient records;
- Banks and bank personnel with respect to bank customer accounts and personal credit information;
- Travel agencies with respect to tourists data;
- School personnel with respect to student records;
- Government agencies and personnel with respect to government records; and
- Insurance personnel with respect to insurance customer information and other insurance records.

Does the law in your jurisdiction restrict or place conditions on the transfer of personal or other information to other foreign jurisdictions?

Chinese laws currently do not place restrictions or conditions on cross-border transfer of information as a general matter. However, there are restrictions that

apply to the transfer of certain types of information (such as the following) to places outside of China.

Personal financial information collected within China by commercial banks must be stored, processed and analysed within the territory of China. Such personal information may not to be transferred overseas unless otherwise permitted by law or regulation.

Similarly, personal information collected by credit reporting agencies within China must be stored and processed within the territory of China, and credit reporting agencies must comply with the law when providing personal information to offshore entities or individuals.

Population health information is also prohibited from being stored in servers abroad.

Furthermore, information containing or concerning state secrets is prohibited from being transferred to places outside China.

Is there a generally applicable obligation to notify data subjects of a data breach in your jurisdiction?

No.

Is there a generally applicable obligation to notify the authorities of a data breach in your jurisdiction?

There is no mandatory requirement under PRC law to report data breaches to any authority as a general matter. However, there are reporting requirements applicable to sectors such as the financial, credit reporting, telecommunications, postal and tax sectors. Please see answer to question below.

Are there sector specific mandatory data breach notification obligations in your jurisdiction?

Yes, a few examples are provided below.

In the financial sector, in the event of a breach concerning any personal financial data, financial institutions are required to promptly report the breach to the People's Bank of China. Also, a commercial bank shall periodically examine the inquiries of the individual credit database and shall report the results of the examination to the People's Bank of China and the credit service centre.

In the event of any actual or potential divulgence or damage or loss of personal information that has caused or may cause serious consequences, telecommunications business operators or internet information service providers must immediately report such event to the relevant telecommunications regulatory authority.

Any company providing postal services or courier services must report to the relevant postal administration authority any information security incident with respect to personal information collected and used in mailing and courier services.

In the event of any leakage of tax-related confidential information of taxpayers, the relevant tax authority must report such event in a timely manner according to relevant laws and regulations.

Howard Wu
Partner, Shanghai
+86 21 6105 8538
howard.wu@bakermckenzie.com

Zhenyu Ruan
Partner, Shanghai
+86 21 6105 8577
zhenyu.ruan@bakermckenzie.com

HONG KONG

Is it unlawful in this jurisdiction to access third party data without authorisation? Is it unlawful to store data which has been accessed without authority?

Accessing third party data without authorisation may constitute offences under various Hong Kong ordinances, summarised below:

- Unauthorised access to a computer by telecommunication: Under section 27A of the Telecommunications Ordinance (Chapter 106 of the Laws of Hong Kong) it is an offence to use telecommunications[1] to affect a computer to obtain unauthorised access to any program or data held in a computer. The offence is punishable by a fine of HK$20,000. This is Hong Kong's "hacking" offence.
- Access to computer with criminal or dishonest intent: Under section 161 of the Crimes Ordinance (Chapter 200 of the Laws of Hong Kong) it is an offence to obtain access to a computer with criminal or dishonest intent to make gain for oneself or another, or to cause loss to another. The offence is punishable by up to five years' imprisonment.

1 "Telecommunications" includes transmission, emission or reception of communication by means of guided or unguided electromagnetic energy or both, other than any transmission or emission intended to be received or perceived directly by the human eye.

- Other property crimes: A person accessing data without authorisation may also be guilty of theft, burglary or fraud under sections 7, 11(3A) and 16A of the Theft Ordinance (Chapter 210 of the Laws of Hong Kong).[2] Further, the offence of destroying or damaging property now also includes "misuse of a computer" (Crimes Ordinance, ss. 59, 60).
- Unauthorised disclosure of personal data: From a data privacy perspective, section 64 of the Personal Data (Privacy) Ordinance (Chapter 486 of the Laws of Hong Kong) makes it an offence to disclose personal data of a data subject obtained from a data user without such data user's consent for purposes of making financial gain or causing financial loss, or to cause psychological harm to the data subject. The offence is punishable by a fine of HK$1,000,000 and up to five years' imprisonment.

There is no specific offence relating to storing data which has been accessed without authority, however, if a person stores data with a view to aiding and abetting the commission of any of the above offences, they may be guilty of conspiracy to commit such offences and would be punishable in the same manner as the relevant offence (Crimes Ordinance, s. 159A).

CIVIL ACTION

Unauthorised access to third party data may also be sufficient basis to initiate civil proceedings against a wrongdoer on a number of possible grounds, including: breach of contract; breach of confidence; trespass to chattel; conversion; misuse of private information; and the economic tort of intentional infliction of harm by unlawful means. Many of these grounds are untested in Hong Kong, but they would at the very least be arguable depending on the circumstances of the unauthorised access.

Is there a legal mechanism whereby you can seek access to or retrieve the copy of data which has been accessed without authority? Is there a legal mechanism that enables you find out information about who may have accessed your data without authority and/or how it was used?

If a data user cannot itself identify who accessed the relevant data and how they used it, the data user can try to obtain this information by working with the Hong Kong Police Force or independent third party forensic investigators.

2 "Property" as defined in section 59 of the Crimes Ordinance includes any program or data held in a computer or a computer storage medium.

For civil actions, there are a number of legal mechanisms by which a data user can procure the assistance of a third party, such as a cloud service provider, to obtain this information, including:

- Norwich Pharmacal Orders: A person who has been wronged may apply to the court for Norwich Pharmacal discovery against any other person who has become involved, directly or indirectly, in the wrongful acts of others so as to facilitate their wrongdoing, whether by voluntary action on his/her part or because it was his/her duty to do as he/she did. The court may order disclosure of the names and addresses of each of the wrongdoers, and other information, so that appropriate remedies can be pursued against the wrongdoer. The cost of complying with Norwich Pharmacal orders is normally borne by the requesting party.
- Anton Pillar Orders: The court may, on application, order the detention, custody and preservation of any property, which is the subject matter of a current or pending civil action or as to which any question may arise in it, or for the inspection of any such property in the possession of a party to the cause or matter. To enable such orders to be carried out, the court may authorise any person to enter upon any land or building in the possession of any party to the action.
- Ex Parte Relief: The court also has the inherent jurisdiction to grant ex parte relief, without notice, authorising the detention, seizure or preservation of property as to which there is strong prima facie evidence that it consists of articles infringing the plaintiff's rights (e.g. copyright, privacy rights), and to make an order that such articles be held in the custody of a responsible person on the plaintiff's behalf.
- Third Party Discovery: Once civil proceedings have commenced, formal discovery may be obtained from persons not party to the proceeding. Parties to an action can apply to the court for an order for discovery against a third party where that third party appears likely to have in its possession, custody or power any document which relates to the matters in the action. Costs of complying with the discovery request will generally be borne by the requesting party.

Is there any restriction on the use that can be made of the information or documentation obtained regarding a data breach incident using a legal process?

Yes, a party obtaining information or documentation pursuant to one of the above described legal processes will be limited to using such information or documentation only for the purposes for which they were obtained. Court orders

will generally specify the limited purposes for which the relevant material is to be used. Any misuse of the material may be restrained by injunction or punishable as a contempt of court.

For documents obtained through the formal discovery of documents process in civil litigation, there is an implied undertaking by a party obtaining such documents to use them only for purposes of conducting its own case, and not for any collateral or ulterior purpose. That party may apply to the court for permission to use the documents for other purposes, such as other proceedings or to disclose the documents to law enforcement authorities, however, such applications will generally only be granted in exceptional circumstances.

Is it possible to maintain confidentiality in relation to the legal steps necessary to get access to the data or information?

Hong Kong civil proceedings are normally held in open court, however, *ex parte* applications for injunctions for orders of a restraining or compulsory nature, such as Anton Pillar or Norwich Pharmacal orders, would not normally be heard in public, particularly if a public hearing would prejudice the interests of justice. Certain matters relating to children, disabled persons and intellectually property rights are also more commonly heard in chambers not open to the public.

When applying for Norwich Pharmacal orders in relation to third party, the applicant may also apply for a "gagging order" prohibiting the third party from disclosing the fact of the application, or compliance with it, to any other party. Gagging orders are generally only made in exceptional circumstances where the court considers there is a demonstrable risk that if the wrongdoer was made aware that he/she was being pursued that he/she would take steps to frustrate any claim or investigation against him/her.

If it is later determined that proceedings should be commenced in another jurisdiction (for example, the perpetrator is found to reside there), can you stop the proceedings in this jurisdiction in such a way that you are not prevented from commencing proceedings on the same issue as a result of the application of res judicata, double jeopardy or some other similar principle?

There is little risk of *res judicata* if no final determination on the merits of the proceeding has been rendered by a Hong Kong court. However, a claimant may encounter procedural obstacles if it undertakes simultaneous civil proceedings on substantially the same issues in two different jurisdictions.

There is no mechanism by which a Hong Kong proceeding can be transferred to a court of another jurisdiction, but a claimant will be free to discontinue the Hong Kong claim with no adverse consequences so long as no final determination of the merits of the claim has been made by the Hong Kong court. Depending on the circumstances, claims can be discontinued either with or without permission of the court.

Claims may be discontinued without the court's permission not later than 14 days after service of a defendant's defence. Discontinuing the claim would not be a bar to the plaintiff bringing another claim in respect of the same cause of action at a later time, however, the defendant will be entitled to his/her taxed (i.e. court assessed) costs.

Claims may be discontinued with the court's permission at any time, but only on terms ordered by the court. The court has broad discretion in making such order and can order that the plaintiff pay the defendant's costs, or not. The court can order that no further action may be brought in respect of the cause of action, or the court may even refuse to grant permission to discontinue the claim and award judgment to the defendant.

Is there an obligation in your jurisdiction to hold personal information securely?

Yes, Data Protection Principle 4 in the Personal Data (Privacy) Ordinance requires that data users take all practical steps to ensure that personal data held by the data user are protected against unauthorised or accidental access, processing, erasure, loss or use. Further, if a data user engages a data processor, whether inside or outside Hong Kong, to process personal data on the data user's behalf, the data user must adopt contractual and other means to keep the data secure.

Various industry regulators have issued guidance and codes of conduct requiring regulated entities to take reasonable steps to implement adequate information security measures, but no concrete standards have yet been mandated.

Does the law in your jurisdiction restrict or place conditions on the transfer of personal or other information to other foreign jurisdictions?

There are no formal requirements under Hong Kong law placing conditions on the transfer of personal data (or other information) to other jurisdictions.

Section 33 of the Personal Data (Privacy) Ordinance does contain restrictions on the circumstances and jurisdictions to which personal data can be transferred outside of Hong Kong, however, this section is not yet in force and there is currently no timeline set for its enforcement.

However, Data Protection Principle 1 does require that data users collecting personal data from data subjects notify them on or before collection of their personal data of not only the purposes for which the data will be put to use, but also the classes of transferees to whom such data may be transferred.

Is there a generally applicable obligation to notify data subjects of a data breach in your jurisdiction?

No. Please see the answer to the next question.

Is there a generally applicable obligation to notify the authorities of a data breach in your jurisdiction?

No, there are no generally applicable mandatory data breach notification obligations in Hong Kong. However, the Privacy Commissioner has issued a *Guidance Note on Data Breach Handling and the Giving of Data Breach Notifications*" which recommends that where personal data is subject to a data breach that notifications be given to the Privacy Commissioner, affected data subjects and various other stakeholders.

Are there sector specific mandatory data breach notification obligations in your jurisdiction?

No, there are no sector specific mandatory data breach notification obligations in Hong Kong. However, various industry regulators do recommend notifications be made in the event of a data breach. For example, the Hong Kong Monetary Authority (HKMA), which regulates banks and other financial institutions, issued its *Guidelines on Customer Data Protection* which indicates that the HKMA expects regulated institutions to report data breaches to the HKMA and affected customers. Although not a prescriptive requirement, failure to meet this expectation could lead to disciplinary sanctions and/or other consequences imposed by the HKMA.

Hong Kong public listed companies are subject to mandatory disclosure requirements in respect of "inside information" which could, if made public, materially affect the price of listed securities: refer s. 307B of the Securities and Futures Ordinance (Chapter 571 of the Laws of Hong Kong). Whether or not a data breach would constitute such inside information is a matter to be addressed by the directors of the listed companies having regard to the specific circumstances of the breach, but such disclosures are currently rare in Hong Kong.

Anna Gamvros
Partner, Hong Kong
+85 22 8462 137
anna.gamvros@bakermckenzie.com

Dominic Wai
Partner, Hong Kong
+85 22 8461 942
dominic.wai@bakermckenzie.com

INDIA

Is it unlawful in this jurisdiction to access third party data without authorisation? Is it unlawful to store data which has been accessed without authority?

As per Section 43 of the *Information Technology Act, 2000* (IT Act), if any person accesses or secures access to a computer, computer system or computer network or resource, without permission of the owner, or person in charge of such computer, he will be liable to pay damages, by way of compensation to the affected person. Further, section 66 of the IT Act states that any person who commits any 'computer related offence' as provided under section 43, will also be punishable by imprisonment for up to three years, or a fine of up to Rs. 5,00,000, or both.

Accordingly, access to third party data stored on a computer, computer network, resource or system is unlawful and punishable under the IT Act.

Also, it may be relevant to discuss the manner in which personal information is dealt with, under the IT Act. The IT Act defines "personal information" to mean "any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (Privacy Rules) further

categorises personal information into a category known as "sensitive personal data or information" (SPDI). SPDI has been defined to mean personal information relating to passwords, financial information, physical or mental health condition, sexual orientation, medical records or biometric information.

As per the IT Act and Privacy Rules, bodies corporate may collect, store, process, dispose of, transfer and use personal information as long as they have notified the person whose data is being collected (Data Subject), the fact that the data is being collected, the purpose and use of such data as well as the intended recipients of the data. In case of personal information amounting to SPDI, the threshold further increases, and express written or electronic consent of the Data Subject is required, prior to collecting, using, processing, transferring, storing or disposing of SPDI. Bodies corporate handling personal information are also required to maintain reasonable security practices and procedures.

Any access or storage of third party personal information, without complying with the requirements under the Privacy Rules would be a violation of section 43A of the IT Act. As per section 43A, where a body corporate possessing, dealing or handling any SPDI in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures, and thereby causes wrongful loss or wrongful gain to any person, such body corporate would be liable to pay damages by way of compensation to the person so affected. The compensation that may be payable is not capped under the IT Act.

Furthermore, non-compliance with the Privacy Rules would generally attract residuary penalty under the IT Act, as per Section 45. Section 45 states that any contravention of the rules or regulations under the IT Act will be penalised with a fine of up to Rs. 25,000.

Is there a legal mechanism whereby you can seek access to or retrieve the copy of data which has been accessed without authority? Is there a legal mechanism that enables you find out information about who may have accessed your data without authority and/or how it was used?

While no specific legal mechanism exists with regard to data breaches, civil courts in India have the power to order discovery by making necessary or reasonable orders for the production, discovery, inspection or impounding of documents or other material which may constitute evidence. Therefore, where the perpetrator is known, an aggrieved individual may approach a civil court and invoke this power to identify the nature, extent and intentions of a data breach.

Is there any restriction on the use that can be made of the information or documentation obtained regarding a data breach incident using a legal process?

No, there is no general restriction on the use that may be made of information or documentation obtained in this regard through a legal process.

Is it possible to maintain confidentiality in relation to the legal steps necessary to get access to the data or information?

As a general rule, court proceedings are open to the public. Only in rare cases do courts exercise their inherent powers to conduct proceedings in private, for example in proceedings involving matrimonial disputes or rape. Indian courts have so far never exercised this discretion with regard to incidents of data breach. However, it would be possible for an aggrieved party to request the court to conduct proceedings in private and restrict publication of consequent orders or judgment.

If it is later determined that proceedings should be commenced in another jurisdiction (for example, the perpetrator is found to reside there), can you stop the proceedings in this jurisdiction in such a way that you are not prevented from commencing proceedings on the same issue as a result of the application of res judicata, double jeopardy or some other similar principle?

Yes, under Indian law the restriction of *res judicata* would only apply where a suit or issue has been previously heard and finally decided by competent court. As such, withdrawing, abandoning or staying legal proceedings prior to final determination would not prevent a party from commencing proceedings in another jurisdiction.

Is there an obligation in your jurisdiction to hold personal information securely?

Yes, under Indian law an entity collecting a Data Subject's "Personal Information" or SPDI (Data Collector) is required to comply with reasonable security practices and procedures. This would require implementation of such security practices, standards and policies that are commensurate with the nature of information being protected. As a part of this requirement, a Data Collector is required to take measures to prevent unauthorised disclosure or transfer of such information.

For the purpose of the above requirements "Personal Information" includes any information that relates to a natural person which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person.

Does the law in your jurisdiction restrict or place conditions on the transfer of personal or other information to other foreign jurisdictions?

Yes, Indian law restricts and regulates the transfer of Personal Information and SPDI to any recipient, including a recipient situated in a foreign jurisdiction.

Transfer of Personal Information or SPDI to a recipient in India or any foreign jurisdiction is permitted provided:

- The recipient ensures the same level of data protection that is adhered to by the Data Collector under Indian law; and
- The transfer:
  - is necessary for the performance of a lawful contract between the Data Collector and the Data Subject; or
  - has been expressly consented to by the Data Subject.

Is there a generally applicable obligation to notify data subjects of a data breach in your Jurisdiction?

No.

Is there a generally applicable obligation to notify the authorities of a data breach in your jurisdiction?

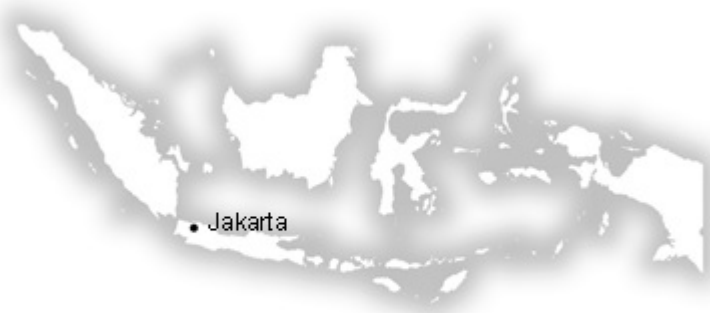
Yes, under the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 all data centers, service providers, intermediaries and companies are required to report certain "cyber security incidents", including unauthorised access of data and IT systems, to the Indian Computer Emergency Response Team (CERT-In).

Such reports are required to be made within reasonable time, so as to leave scope for appropriate action by the authorities. The format and procedure for reporting of cyber security incidents have been provided by Cert-In on its official website, http://www.cert-in.org.in/

Are there sector specific mandatory data breach notification obligations in your jurisdiction?

No.

Sajai Singh
Partner, J. Sagar Associates
+91 80 435 03600
sajai@jsalaw.com



INDONESIA

Is it unlawful in this jurisdiction to access third party data without authorisation? Is it unlawful to store data which has been accessed without authority?

Yes. Under article 32 of the Law of the Republic of Indonesia Number II of 2008 concerning Electronic Information and Transactions Law(EIT Law):

> Each person is prohibited, whether intentionally and without right or unlawfully, from changing, adding, reducing, transmitting, destroying, deleting, transferring or hiding in any way electronic information and/or electronic documents belonging to other persons.
>
> Each person is prohibited, whether intentionally and without right or unlawfully, from moving or transferring electronic information and/or electronic documents to another person.
>
> Each person is prohibited, whether intentionally and without right or unlawfully, from committing the act as referred to in point (a) if that causes confidential electronic information and/or electronic documents to become accessible by the public.

Violation of the above provisions may result in imprisonment of up to 10 years and/or monetary fines up to Rp. 5,000,000,000.

Further, under the EIT Law and Government Regulation (GR) 82, any use of personal data (e.g. collect, process, disclose, transfer, etc) must be based on consent from the relevant data owner and that use of personal data must be in accordance with the purpose conveyed to the data owner when collecting the personal data. Consequently, any unauthorised access or storage of personal data is unlawful.

In addition to the EIT Law, article 322.1 of the Indonesian Criminal Code also provides that anyone who intentionally discloses confidential information that he/she is under an obligation to keep secret by virtue of his/her present or past position or employment is subject to nine months imprisonment.

A violation of GR 82 may also result, where the relevant party is a legal entity, in administrative sanctions in the form of warning letters, administrative fines, suspension, and deregistration as a business.

Is there a legal mechanism whereby you can seek access to or retrieve the copy of data which has been accessed without authority? Is there a legal mechanism that enables you find out information about who may have accessed your data without authority and/or how it was used?

There is no specific legal mechanism in relation to a data breach. However, the matter could be referred to the police and/or other relevant institutions (e.g. District Attorney and the Minister of Communications and Informatics) in the case of criminal proceedings and based on reports for the relevant authorities to conduct investigations and identify any relevant matter (e.g. who may have accessed the data, how it was used and/or other relevant matters in relation to the alleged violation or breach).

Is there any restriction on the use that can be made of the information or documentation obtained regarding a data breach incident using a legal process?

Generally, in Indonesia, all proceedings are open to the public (except for several matters such as family and child proceedings, etc) and any information or documentation obtained from such proceeding (including the court judgments) is also available to the public and can be used for any purposes. In reality though gaining public access is very difficult and rarely done and judgments are not readily available.

Is it possible to maintain confidentiality in relation to the legal steps necessary to get access to the data or information?

No, as noted above the general rule is that all proceedings are open to the public (except for several matters such as family and child proceedings, etc) as determined by the relevant Court).

If it is later determined that proceedings should be commenced in another jurisdiction (for example, the perpetrator is found to reside there), can you stop the proceedings in this jurisdiction in such a way that you are not prevented from commencing proceedings on the same issue as a result of the application of res judicata, double jeopardy or some other similar principle?

It is not possible to do so in the case of criminal proceedings. However, it may be possible to do so in the case of a civil proceeding provided that there has been no

court judgment for that case and the relevant claim is revoked by the plaintiff before the defendant filed any response to the claim.

Is there an obligation in your jurisdiction to hold personal information securely?

Yes. As a general rule, under GR 82, Electronic Systems Operators must:

- maintain the secrecy, integrity, and availability of personal data that is being managed;
- ensure that the collection and use of personal data is based on the personal data subject's consent, unless otherwise provided by laws and regulations; and
- ensure that the use or disclosure of data is with the personal data subject's consent, and in accordance with the purpose for the data collection conveyed to the personal data subject.

Does the law in your jurisdiction restrict or place conditions on the transfer of personal or other information to other foreign jurisdictions?

Not specifically. However, as noted above, any use of personal data (including transfer of data) must be done with the data subject's consent.

Is there a generally applicable obligation to notify data subjects of a data breach in your Jurisdiction?

Yes, GR 82 requires written notification to the relevant data subjects in case of a data breach. However, there is no specific procedure or timeline in relation to the notification.

Is there a generally applicable obligation to notify the authorities of a data breach in your jurisdiction?

No.

Are there sector specific mandatory data breach notification obligations in your jurisdiction?

No.

Mark Innis
Partner, Jakarta
+62 21 2960 8618
mark.innis@bakernet.com

Alvira M Wahjosoedibjo
Partner, Jakarta
+62 21 2960 8503
alvira.m.wahjosoedibjo@bakernet.com

JAPAN

Is it unlawful in this jurisdiction to access third party data without authorisation? Is it unlawful to store data which has been accessed without authority?

Yes. Under the Act on Prohibition of Unauthorized Computer Access, engaging in "Unauthorized Computer Access", which is defined to mean access to a computer by circumventing access restrictions set up for the said computer, is prohibited. Accordingly, an unauthorised use of other peoples' passwords and attacking the computer through its vulnerability (e.g. defect in the security programs or erroneous setting in security control) typically fall within Unauthorized Computer Access.

Storage of data obtained through unauthorised access is not a crime or illegal act under Japanese laws, but usage or disclosure of the data can constitute unfair competition defined under the Unfair Competition Prevention Act if the data falls under a "Trade Secret".

Both of the unauthorised access and usage or disclosure of the data obtained through unauthorised access can trigger civil liability based upon general tort laws and the Unfair Competition Prevention Act.

Is there a legal mechanism whereby you can seek access to or retrieve the copy of data which has been accessed without authority? Is there a legal mechanism that enables you find out information about who may have accessed your data without authority and/or how it was used?

Yes. If the identity of the party who accessed the data or who owns the data is already known, there are some options to demand the party disclose the relevant data concerning the unauthorised access.

If the data in question is maintained by entities (e.g. governmental organisation, business enterprises), a Japanese qualified attorney can request the entity to disclose the data if the disclosure is necessary to resolve the case for which the attorney is retained.

This is a legal mechanism called "23 Jou Shokai" (or Article 23 Inquiry). To make this request of 23 Jou Shokai, the attorney shall submit the written request to the Bar Association to which he or she belongs, and the Bar Association will send the request to the entity specified in the attorney's request. The entities which receive the request are generally required to disclose the requested information.

In a civil litigation, it is possible to leverage a "Document Submission Order" issued by the court.

Under the Japanese Civil Code, the court has the authority to order the owner of documents (including but not limited to the party to the litigation) to submit the documents as evidence upon the party's petition (Document Submission Order). If the order is issued against either of the parties to the litigation and the party does not comply with the order, the court can deem the other party's argument concerning the document to be true.

In principle, the petitioner must identify the subject document by the type, title, date, author or writer or other specific information of the document in the petition. However, if the specific information is not available to the petitioner, the petitioner can file the petition without the specific information as long as the petition provides information which enables the document owner to identify the subject document.

Is there any restriction on the use that can be made of the information or documentation obtained regarding a data breach incident using a legal process?

Yes. Attorneys are prohibited from using 23 Jou Shokai for any purposes other than resolving the case which he or she handles. Therefore, for example, using customer data obtained through 23 Jou Shokai for business not related to the dispute is prohibited.

With respect to evidence submitted to the court in a litigation (including those submitted pursuant to the Document Submission Order) concerning patent, trademark trade secret or copyright, the court may issue a confidentiality order, which prohibits the parties to the litigation, its attorney, employees, and agents etc. from using the information for any purpose other than the litigation if the information constitutes a trade secret under Japanese laws.

Is it possible to maintain confidentiality in relation to the legal steps necessary to get access to the data or information?

Yes. A party to a litigation concerning intellectual property rights can file a petition to the court to issue a confidentiality order as mentioned above.

Another means is to file a petition to restrict access to the case record. Due to a constitutional requirement, case records are generally accessible by the public, however, if the record contains important, private confidential information or a trade secret, upon the party's petition, the court can restrict the general public's access to the confidential information or trade secret in the case records. Even before the court issues its decision to restrict access, the court tentatively restricts the access to such information automatically once the petition is filed.

If it is later determined that proceedings should be commenced in another jurisdiction (for example, the perpetrator is found to reside there), can you stop the proceedings in this jurisdiction in such a way that you are not prevented from commencing proceedings on the same issue as a result of the application of res judicata, double jeopardy or some other similar principle?

Yes. A plaintiff can withdraw its complaint freely before the defendant responds to the action at the court or submits an answer to the court. After the defendant's response or submission of an answer, the plaintiff needs to obtain the defendant's consent to withdraw the complaint. Withdrawal is permitted even after the court issues its judgment as long as the defendant consents.

The Japanese Civil Procedure Code prohibits filing another action which is the same as what was withdrawn after the issuance of the judgment in the prior case. In other words, litigation in another jurisdiction after the withdrawal is not prohibited if the prior action was withdrawn before the court issues the judgment.

The Japanese Civil Procedure Code also authorises the court to transfer the case with or without the party's petition for transfer, when certain requirements are met. Once the court's order to transfer the case becomes effective and binding, the case is deemed to have been pending before the court to which the case was transferred.

Is there an obligation in your jurisdiction to hold personal information securely?

Yes. According to the Act on Protection of Personal Information (the "APPI"), governing data privacy in Japan, any individual or entity who maintains and manages personal data of more than 5,000 individuals for its business must take

necessary and appropriate measures to prevent leakage, loss or damage of the personal information and otherwise ensure security management of the personal information. While the language of the act in this respect is relatively broad, the security requirement is detailed in industry-specific guidelines released by several governmental authorities.

Does the law in your jurisdiction restrict or place conditions on the transfer of personal or other information to other foreign jurisdictions?

No. The current APPI does not prevent data controllers from transferring the personal information to other jurisdictions. If the transfer involves transfer of personal information to a third party, it requires consent from the data subject unless the transfer falls within any of the exceptions set forth in the APPI. However, the current rules on transfer of personal information do not vary depending on whether the personal information is transferred to foreign jurisdictions or not.

It should be noted, however, the bill of amendments to the APPI that the congress is discussing (submitted to the congress on 10 March 2015) states that transfer of personal information to third parties located outside Japan in principle requires consent from the data subject.

Is there a generally applicable obligation to notify data subjects of a data breach in your Jurisdiction?

There is no express provision in the APPI creating an obligation to notify data subjects in the event of a data security breach.

However, some of the sector specific guidelines published by governmental authorities state that the data controllers must notify the data subjects promptly upon a data security breach. In addition, the prompt notification of data subjects and the public announcement of a data security breach may help minimise existing and future damages to the affected data subjects so that, in turn, may also help to minimise the data controller's potential obligation to compensate the data subjects for damages incurred.

Is there a generally applicable obligation to notify the authorities of a data breach in your jurisdiction?

There is no express provision in the APPI creating an obligation to notify the authorities in the event of a data security breach.

However, competent ministries have the authority to collect reports from, advise, instruct, or give orders to the data controllers, and, as a result, the data controller may be required by competent ministries to notify the data subjects and/or competent ministries in the event of a data security breach within a specific time frame in accordance with ministerial orders.

Are there sector specific mandatory data breach notification obligations in your jurisdiction?

Yes. Some of the sector specific guidelines create an obligation to notify the governmental authorities promptly upon occurrence of a data security breach. For example, according to the guidelines issued by the Financial Service Agency, banking and other financial businesses need to take such action in the event of a data security breach in accordance with the relevant guidelines.

Daisuke Tatsuno
Partner, Tokyo
+81 3 6271 9479
daisuke.tatsuno@bakermckenzie.com

Nobuko Narita
Senior Counsel, Tokyo
+81 3 6271 9732
nobuko.narita@bakermckenzie.com

MALAYSIA

Is it unlawful in this jurisdiction to access third party data without authorisation? Is it unlawful to store data which has been accessed without authority?

There are a number of criminal offences in relation to unauthorised access of electronic data, which carry prison sentences. The severity of the offence is related to the intention of the perpetrator in accessing and using the data. For example, if the data is accessed for purposes of committing a further crime such as fraud or dishonesty, the punishment is more severe.

Persons who aid, abet, counsel, or procure someone to commit a criminal offence have also committed a criminal offence.

In addition, under the *Malaysian Personal Data Protection Act, 2010* (PDPA) which came into force in late 2013, the collection or disclosure of personal data held by a data user, without the consent of the data user, also amounts to a criminal offence which carries a monetary fine and/or imprisonment.

In terms of civil actions, if the data accessed is confidential, there may also be claims available in contract (if there is a contractual obligation to keep the data confidential, which is common place in many employment or business contracts) or in equity for breach of confidence (if the confidential information is improperly obtained or imparted in a manner which requires it not to be divulged). If a person is asked to store data which they know to have been obtained improperly, a claim may also be made against them for a breach of confidence.

The PDPA does not provide data users/data subjects with civil remedies.

Is there a legal mechanism whereby you can seek access to or retrieve the copy of data which has been accessed without authority? Is there a legal mechanism that enables you find out information about who may have accessed your data without authority and/or how it was used?

If the identity of the person(s) who either committed the data breach or are storing or have stored the data at some point in time is known, the matter could

be referred to the police and/or civil proceedings could be commenced. There are two civil processes which may be appropriate depending on the circumstances: search and seizure orders and / or preliminary discovery.

An Anton Piller Order is possible where there is a grave danger the defendant will dispose of or destroy incriminating evidence in its possession or control before trial, and its continued existence is necessary for the plaintiff's case. The order is usually made *ex parte* and enables the plaintiff and/or its representatives to enter the defendant's premises to search for, inspect and seize or make copies of materials so that they may be preserved until trial.

Generally, the Malaysian Courts also have the discretion to order discovery of documents prior to trial. Generally speaking, such order would only be granted in rare or exceptional circumstances.

If civil proceedings for breach of confidentiality obligations are brought and are ultimately successful, one of the orders made may be for the delivery up of the data accessed, damages or any account of profits.

Is there any restriction on the use that can be made of the information or documentation obtained regarding a data breach incident using a legal process?

Yes, there is a general obligation on parties to only use the documents for purposes of proceedings in which they are produced.

Is it possible to maintain confidentiality in relation to the legal steps necessary to get access to the data or information?

Generally no, as every document that is filed in the Malaysian Court can be accessed by the public through file searches at the relevant Court. Documents containing matters confidential to a party and not otherwise privileged must be disclosed, but the Court may order a controlled method of disclosure to protect confidentiality.

If it is later determined that proceedings should be commenced in another jurisdiction (for example, the perpetrator is found to reside there), can you stop the proceedings in this jurisdiction in such a way that you are not prevented from commencing proceedings on the same issue as a result of the application of res judicata, double jeopardy or some other similar principle?

Yes, but only if the issues and/or matters in relation to the proceedings have not been conclusively determined. Potential issues could arise if proceedings are being conducted concurrently in two jurisdictions on the same subject matter.

Is there an obligation in your jurisdiction to hold personal information securely?

Yes. The Security Principle of the PDPA requires that a data user shall take practical steps to protect personal data from any loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction by having regard to:

- the nature of the personal data and the harm that would result from such loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction;
- the place or location where the personal data is stored;
- any security measures incorporated into any equipment in which the personal data is stored;
- the measures taken for ensuring the reliability, integrity and competence of personnel having access to the personal data; and
- the measures taken for ensuring the secure transfer of the personal data.

The Personal Data Protection Regulations 2013 (Regulations) further elaborates on the Security Principle whereby a "data user shall develop and implement a security policy which complies with the security standards as set out from time to time by the Commissioner". At present, no such security standards have been issued. Based on feedback from the Malaysian Personal Data Protection Department (Regulator), the implementation of and adherence to, the Security Principle is, at present, self-regulatory in nature. It is left to the data user to determine how the data user develops, implements, and ensures the security of the personal data processed.

Does the law in your jurisdiction restrict or place conditions on the transfer of personal or other information to other foreign jurisdictions?

The PDPA provides that personal data shall not be transferred outside of Malaysia unless it is to a place specified by the Minister. The Minister has not yet specified such places. The PDPA does however provide for circumstances (Exceptions) where personal data may be so transferred outside of Malaysia.

The Exceptions are set out below:

- The data subject has given his or her consent to the transfer;
- The transfer is necessary for the performance of a contract between the data subject and data user;

- The transfer is necessary for the conclusion or performance of a contract between the data user and a third party which (i) is entered into at the request of the data subject; or (ii) is in the interests of the data subject;
- The transfer is for the purpose of any legal proceedings or for the purpose of obtaining legal advice or for establishing, exercising or defending legal rights;
- The data user has reasonable grounds for believing that in all circumstances of the case (i) the transfer is for the avoidance or mitigation of adverse action against the data subject; (ii) it is not practicable to obtain the consent in writing of the data subject to that transfer; and (iii) if it was practicable to obtain such consent, the data subject would have given his or her consent;
- The data user has taken all reasonable precautions and exercised all due diligence to ensure that the personal data will not be processed in that place in any manner which, if that place is Malaysia, would be a contravention of the PDPA;
- The transfer is necessary in order to protect the vital interests of the data subject; or
- The transfer is necessary as being in the public interest in circumstances as determined by the Minister.

Is there a generally applicable obligation to notify data subjects of a data breach in your jurisdiction?

Generally, no. The PDPA is also silent on this issue. It is however possible that the Regulator may take such notification into account in determining whether the data user has complied with the Security Principle under the PDPA. Formal codes of practice have yet to be issued on this matter.

Is there a generally applicable obligation to notify the authorities of a data breach in your jurisdiction?

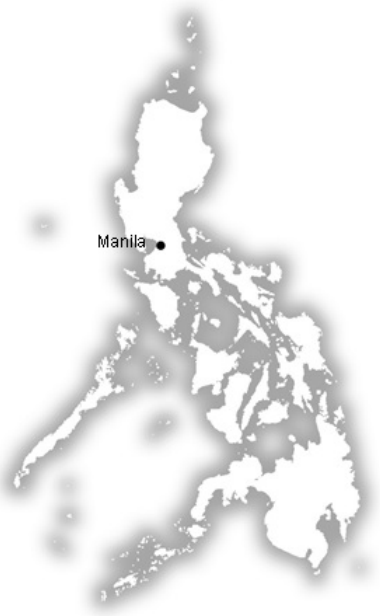
Generally, no. The PDPA is also silent on this issue. It is however possible that the Regulator may take such notification into account in determining whether the data user has complied with the Security Principle under the PDPA. Formal codes of practice have yet to be issued on this matter.

Are there sector specific mandatory data breach notification obligations in your jurisdiction?

No. However, this may be addressed in the formal codes of practice which are intended to be issued to supplement the provisions of the PDPA.

Wei Kwang Woo
Partner, Kuala Lumpur
+60 32 2987898
weikwang.woo@wongpartners.com

Adrian Wong
Senior Associate, Kuala Lumpur
+60 32 2987952
adrian.wong@wongpartners.com



PHILIPPINES

Is it unlawful in this jurisdiction to access third party data without authorisation? Is it unlawful to store data which has been accessed without authority?

Accessing third party data without authorisation may be unlawful under several laws in the Philippines.

If the data is accessed and stored by a third party without authorisation from the owner of the data, the access and storage may be considered to be an offence punishable under the *Cybercrime Prevention Act of 2012 (Republic Act No. 10175*; "Cybercrime Act") for being an offense against the confidentiality, integrity and availability of computer data and systems. Depending on the nature and scope of the act perpetrated, the unauthorised access may be classified as any of the following offences:

Illegal Access – The access to the whole or any part of a computer system without right.

Illegal Interception – The interception made by technical means without right of any non-public transmission of computer data to, from, or within a computer system including electromagnetic emissions from a computer system carrying such computer data.

Data Interference — The intentional or reckless alteration, damaging, deletion or deterioration of computer data, electronic document, or electronic data message, without right, including the introduction or transmission of viruses.

System Interference — The intentional alteration or reckless hindering or interference with the functioning of a computer or computer network by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data or program, electronic document, or electronic data message, without right or authority, including the introduction or transmission of viruses.

Misuse of Devices:

- The use, production, sale, procurement, importation, distribution, or otherwise making available, without right, of:
  - A device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences under the Cybercrime Act; or
  - A computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed with intent that it be used for the purpose of committing any of the offences under this Act.
- The possession of an item referred to in subparagraphs (a)(i) and (a)(ii) above with intent to use said devices for the purpose of committing any of the offences above.

When the information accessed involves personal data, the Data Privacy Act of 2012 (Republic Act No. 10173, "DPA") penalises the unauthorised access or intentional breach by persons who knowingly and unlawfully, or violating data confidentiality and security data systems, breaks in any way into any system where personal and sensitive personal information is stored.

Is there a legal mechanism whereby you can seek access to or retrieve the copy of data which has been accessed without authority? Is there a legal mechanism that enables you find out information about who may have accessed your data without authority and/or how it was used?

The Cybercrime Act has provisions that mandate a service provider to preserve computer data (integrity of traffic data and subscriber information). Content data shall be preserved upon receipt of a request from law enforcement authorities requiring their preservation. The preserved data will then be accessed or disclosed after securing a court warrant (search warrant) to disclose or submit subscriber's information, traffic data or relevant data in the service provider's possession or control. In turn, the disclosed information may reveal information as to what data has been accessed, who accessed the information and how the information was subsequently used.

If the illegally accessed, retrieved or copied data involves personal information, the DPA mandates (among other responsibilities of a personal information controller/service provided) that the personal information controller/service provider notify the affected data subject. The notification shall at least describe the nature of the breach, the personal information possibly involved, and the measures taken to address the breach.

Is there any restriction on the use that can be made of the information or documentation obtained regarding a data breach incident using a legal process?

We are not aware of any law or regulation which specifically restricts the use of information or documentation obtained regarding a data breach incident. Anton Piller orders[3] are not recognized in the Philippines. However, as discussed in the first paragraph in the previous question, the Cybercrime Act mandates a service provider to preserve the integrity of traffic data and subscriber information relating to communication services (law requires preservation for a minimum period of six months). Upon request of a law enforcement authority, content data may similarly be preserved.

Is it possible to maintain confidentiality in relation to the legal steps necessary to get access to the data or information?

The Cybercrime Act requires service providers to preserve traffic data (any computer data other than the content of the communication including, but not limited to, the communication's origin, destination, route, time, date, size, duration, or type of underlying service) for a period six months from the date of the data transaction. Law enforcement authorities may order a one-time extension for another six months subject to the conditions set out in the law.

In this procedure, the service provider (which was ordered to preserve computer data) is mandated by law to keep the order, and its compliance, confidential.

If it is later determined that proceedings should be commenced in another jurisdiction (for example, the perpetrator is found to reside there), can you stop the proceedings in this jurisdiction in such a way that

3 is a court order that provides the right to search premises and seize evidence without prior warning. This prevents destruction of relevant evidence, particularly in cases of alleged trademark, copyright or patent infringements. Note that Section 19 of the Cybercrime Act would have created an Anton Piller type power for the Department of Justice upon *prima facie* information that a computer data is found to violate provisions of the Act. However, Section 19 was declared unconstitutional by the Philippine Supreme Court.

you are not prevented from commencing proceedings on the same issue as a result of the application of res judicata, double jeopardy or some other similar principle?

It may be argued that legal proceedings in another jurisdiction should not affect the remedies available to persons subject to the jurisdiction of Philippine law. In this context, any proceedings initiated in another jurisdiction should, strictly speaking, not affect the jurisdiction (nor the proceedings, if already initiated) in the Philippines. In the same line of reasoning, the legal concepts of *res judicata* or double jeopardy, should not apply.

Is there an obligation in your jurisdiction to hold personal information securely?

Yes. The DPA requires that personal information controllers must implement reasonable and appropriate organisational, physical and technical measures intended for the protection of personal information against any accidental or unlawful destruction, alteration and disclosure, as well as against any other unlawful processing.

Further, personal information controllers must implement reasonable and appropriate measures to protect personal information against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration and contamination.

Does the law in your jurisdiction restrict or place conditions on the transfer of personal or other information to other foreign jurisdictions?

The DPA states that each personal information controller is responsible for information that has been transferred to a third party for processing internationally. The personal information controller is accountable for complying with the requirements of the DPA and shall use contractual or other reasonable means to provide a comparable level of protection while the information is being processed by a third party in a foreign jurisdiction.

Further, Presidential Decree 1718 (PD 1718), in general, regulates the transfer of information to locations outside of the Philippines in limited circumstances, particularly when the information deals with information considered as "vital to the national interest".

Is there a generally applicable obligation to notify data subjects of a data breach in your Jurisdiction?

The DPA imposes an obligation for the personal information controller to notify data subjects (and the National Privacy Commission) of a data breach in one instance: when sensitive personal information that may, under the circumstances, be used to enable identity fraud is reasonably believed to have been acquired by an unauthorised person, and the personal information controller or the National Privacy Commission believes that such unauthorised acquisition is likely to give rise to a real risk of serious harm to any affected data subject.

Is there a generally applicable obligation to notify the authorities of a data breach in your jurisdiction?

Please see our response above.

Are there sector specific mandatory data breach notification obligations in your jurisdiction?

For banking and banking related services, the Bangko Sentral ng Pilipinas (Central Bank of the Philippines; "BSP") issued Circular No. 808 (Series of 2013) which covers Guidelines on Information Technology Risk Management for All Banks and Other BSP Supervised Institution. Part of the guidelines include an obligation to "report any breach in information security, especially incidents involving the use of electronic channels" to the BSP.

Bienvenido Marquez
Partner, Manila
+63 2 819 4936
bienvenido.marquez@quisumbingtorres.com

SINGAPORE

Is it unlawful in this jurisdiction to access third party data without authorisation? Is it unlawful to store data which has been accessed without authority?

Yes. Under the Personal Data Protection Act 2012 (PDPA), it is an offence to collect personal data without the data subject's consent, unless an exception applies. It is also an offence under the PDPA for a person to make a request to obtain access to or to change the personal data about another individual, which is in the possession or under control of an organisation, without the authority of that individual.

Under the Computer Misuse and Cybersecurity Act (CMCA), it is an offence to knowingly cause a computer to perform any function for the purpose of securing access without authority to any data held in any computer.

Further, a plaintiff may make a claim under tort for, amongst others, conversion or breach of a duty of confidentiality.

Is there a legal mechanism whereby you can seek access to or retrieve the copy of data which has been accessed without authority? Is there a legal mechanism that enables you find out information about who may have accessed your data without authority and/or how it was used?

There are various possible mechanisms, depending on the circumstances:

- The matter may be referred to the police for criminal prosecution via a complaint. While the assistance of the police may be sought, the complainant strictly has no control over the conduct of the matter by the police and has

no right to request information or documents from the police. It is within the police's discretion whether it chooses to reveal anything to the complainant.

- Civil proceedings for, amongst others, breach of confidence may also be commenced. As part of the final relief in such civil proceedings, the complainant may seek an injunction for the delivery up, return and/or deletion of the data which has been accessed without authority, damages and/or an account of profits. There are also various interim measures or forms of injunctive relief available, for example:
  - an application for a search and seizure order, for permission to search, inspect and either copy or remove documents in the possession of the defendant(s), when there is (amongst other requirements) a grave danger that the defendant(s) will dispose of or destroy incriminating evidence in his/her possession. These documents which are seized are not ordinarily provided to the plaintiff immediately, but an order may be made for inspection by the plaintiff of those documents;
  - an application for interim injunction to, amongst other things, restrain the defendant(s) from using and/or disclosing such data pending the final resolution of the civil proceeding;
  - the process of general and/or specific discovery, interrogatories and/or further and better particulars of pleadings, may be applicable.
  - If the identity of the person who either committed the data breach or is storing or has stored the data at some point in time is unknown and/or civil proceedings have not been commenced, the complainant may make an application for pre-action discovery or pre-action interrogatories against known parties who may be involved. Such applications, if successful, may require an individual or company to produce documents or answer questions so that either the identity of the potential defendant(s) may be determined or the plaintiff can assess whether there is a case to be made.

Is there any restriction on the use that can be made of the information or documentation obtained regarding a data breach incident using a legal process?

Yes. There is a general rule that a party who obtains documents from the other party under compulsion (for example in discovery of documents in Court proceedings) may only use such documents for the conduct of his/her case, and that party is under an implied undertaking that he/she will not use the documents for any other purpose.

In Singapore, there is some uncertainty about whether this implied undertaking ceases to apply once the document has been used in open court. In a recent High Court decision, the Court held that this is the case, but the party who discloses the document or the party who owns the document may apply to the court for the implied undertaking to continue. It remains to be seen whether this decision will be upheld by the Singapore Court of Appeal.

Is it possible to maintain confidentiality in relation to the legal steps necessary to get access to the data or information?

Ordinarily no, but in some narrow circumstances a party may apply to the Court to seal the file or hold proceedings in private in order to keep the proceedings or their subject matter confidential. The Court's jurisdiction to seal the file or hold proceedings in private arises out of its inherent jurisdiction, and the Court will only exercise such jurisdiction in exceptional cases.

If it is later determined that proceedings should be commenced in another jurisdiction (for example, the perpetrator is found to reside there), can you stop the proceedings in this jurisdiction in such a way that you are not prevented from commencing proceedings on the same issue as a result of the application of res judicata, double jeopardy or some other similar principle?

Withdrawing, discontinuing or staying Singapore proceedings before the final determination of the action generally does not prevent a plaintiff from commencing subsequent proceedings either in Singapore again, or in another jurisdiction, for the same or substantially the same cause of action, unless the Court orders otherwise. However, if a particular issue has been heard and determined before such withdrawal, discontinuance or stay (for example, an issue in a preliminary determination), an argument may be raised that the parties are estopped from reopening that issue in Singapore or in another jurisdiction. Further, there may also be an issue if proceedings are actively occurring in two jurisdictions at the same time which cover the same issue(s).

Whether the withdrawal, discontinuance or staying of the Singapore proceeding(s) has the effect of preventing one of the parties from commencing subsequent proceedings on the same issue will also depend on the laws of the other jurisdiction where the proceeding(s) may subsequently be commenced.

Is there an obligation in your jurisdiction to hold personal information securely?

Yes. Organisations must ensure that they 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.

Does the law in your jurisdiction restrict or place conditions on the transfer of personal or other information to other foreign jurisdictions?

Yes. Organisations must not transfer personal data outside of Singapore except in accordance with requirements prescribed under the PDPA to ensure that organisations provide a standard of protection to the transferred personal data that is comparable to the protection under the PDPA. This would include entering into binding corporate rules or intercompany agreements.

Further, banking secrecy laws place certain restrictions on the disclosure of customer information by licensed banks in Singapore.

Is there a generally applicable obligation to notify data subjects of a data breach in your Jurisdiction?

No.

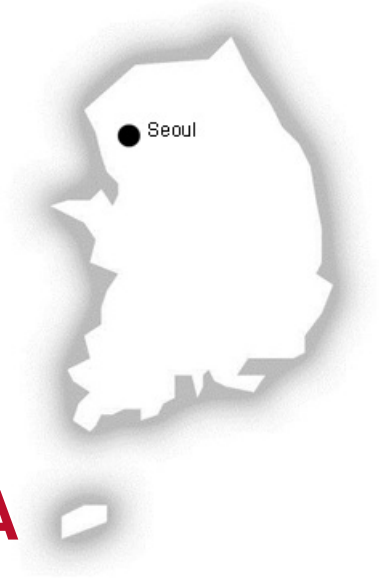
Is there a generally applicable obligation to notify the authorities of a data breach in your jurisdiction?

No.

Are there sector specific mandatory data breach notification obligations in your jurisdiction?

Yes, regulated financial institutions must notify the Monetary Authority of Singapore as soon as possible, but not later than one hour, upon the discovery of a "relevant incident", which includes IT security incidents which have a severe and widespread impact on the financial institution's operations or materially impacts the financial institution's service to its customers.

Ken Chia
Partner, Singapore
+65 6 434 2558
ken.chia@bakermckenzie.com



SOUTH KOREA

Is it unlawful in this jurisdiction to access third party data without authorisation? Is it unlawful to store data which has been accessed without authority?

Under the Personal Information Protection Act (the "PIPA"), a personal information manager who collects personal information of a person without having obtained the consent of the subject person may be subject to an administrative fine of up to KRW 50 million. If a personal information manager damages, destroys, alters, fabricates or leaks personal information of others, the personal information manager may be subject to imprisonment for up to two years or a fine of up to KRW 10 million. For the purposes of the PIPA, the personal information manager means an entity or individual that manages the processing of personal information for itself/himself/herself or through another entity or person to operate personal information files for business purposes. The personal information manager under the PIPA is more like a data controller rather than a data processor under the EU's legislative system.

In addition, if the relevant personal information is secret information, the personal information manager may be subject to imprisonment or imprisonment without forced labor for up to three years or a fine of up to KRW five million for violation of secrecy under the Criminal Code.

Under the Act on Promotion of Information and Communications Network Utilization and Information Protection (the "Information and Communications Network Act"), no one shall damage another person's information processed, stored or transmitted through an information and communications network, nor

shall infringe, misappropriate or leak another person's secret. A violation of the above provision may result in imprisonment for up to five years or a fine of up to KRW 50 million.

Under the Information and Communications Network Act, no one shall collect another person's information or induce another person to furnish information through an information and communications network by fraud. A violation of the above provision may result in imprisonment for up to three years or a fine of up to KRW 30 million.

The PIPA, the Information and Communications Network Act, the Act on Use and Protection of Credit Information (the "Credit Information Act"), the Act on Use and Protection of Location Information, etc. contain provisions of liability for damage compensation in connection with personal information protection.

Is there a legal mechanism whereby you can seek access to or retrieve the copy of data which has been accessed without authority? Is there a legal mechanism that enables you find out information about who may have accessed your data without authority and/or how it was used?

If a person reports a data breach to a data breach complaint centre established based on the PIPA or the Information and Communications Network Act (the "Complaint Centre"), the Complaint Centre may demand that the relevant personal information manager or information and communications service provider submit documents and other materials related to the data breach in question. The Complaint Centre is required to conduct a fact-finding investigation for such a data breach and upon the completion of the fact-finding investigation, notify the person who made the report of the results of the fact-finding investigation and of the measures taken with respect to the data breach.

If a victim of a data breach files a civil claim for damage compensation with a court, the person may petition the court to grant an order for production of documents, whereby materials related to the data breach in question may be obtained.

Is there any restriction on the use that can be made of the information or documentation obtained regarding a data breach incident using a legal process?

Under the Civil Procedure Act, a party may petition the court to limit the persons who are eligible to make a request for access to litigation documents which contain secrets to the parties to the litigation. Other than that, there are no particular restrictions.

Is it possible to maintain confidentiality in relation to the legal steps necessary to get access to the data or information?

Under the Civil Procedure Act, when a person or an entity submits certain documents pursuant to a court order for production of documents, such a person or an entity may request an in private examination of the submitted documents.

If it is later determined that proceedings should be commenced in another jurisdiction (for example, the perpetrator is found to reside there), can you stop the proceedings in this jurisdiction in such a way that you are not prevented from commencing proceedings on the same issue as a result of the application of res judicata, double jeopardy or some other similar principle?

If the lawsuit is withdrawn before the court renders a final decision, you can subsequently commence proceedings on the same issue. If the lawsuit is withdrawn after the court has rendered a final decision, you are prevented from commencing proceedings on the same issue based on the principle of *res judicata*. You are prevented from commencing proceedings on the same issue when proceedings on the same issue are pending and not withdrawn (based on the principle of prohibition against double jeopardy).

Is there an obligation in your jurisdiction to hold personal information securely?

The PIPA imposes personal information protection obligations on the personal information managers, and the Information and Communications Network Act imposes personal information protection obligations on the information and communications service providers.

Does the law in your jurisdiction restrict or place conditions on the transfer of personal or other information to other foreign jurisdictions?

Under the Information and Communications Network Act, an information and communications service provider should not enter into an international contract containing any term or condition that violates the Information and Communications Network Act with respect to users' personal information, and for an overseas transfer of users' personal information, should notify the subject users of certain matters and obtain the consent of each such user. In addition, when an information and communications service provider intends to transfer users' personal information overseas after having obtained the consent of the users, the information and communications service provider is required to take certain protective measures as prescribed by the Information and Communications Network Act and the Enforcement Decree thereto.

Under the PIPA, a transfer of personal information to an overseas third party requires the notification of certain matters to the data subjects and the consent of the data subjects, as in the case of a provision of personal information to a third party in Korea. Entering into an agreement for overseas transfer of personal information that would violate the above provision is prohibited.

Is there a generally applicable obligation to notify data subjects of a data breach in your Jurisdiction?

Under the PIPA, in the event of a data breach, the personal information manager is required to promptly notify the data subjects of the details of such a data breach.

Under the Information and Communications Network Act, if an information and communications service provider becomes aware of a loss, theft or leak of personal information, the information and communications service provider is required to notify the relevant users of certain matters concerning such event (as prescribed by the Information and Communications Network Act), and to report to the Korea Communication Commission or the Korea Internet & Security Agency, which notification and report, without any justifiable reason, must not be made after the lapse of 24 hours from the time when the communications service provider becomes aware of such event. This reporting obligation is absolute. The notification and report may be made after the lapse of 24 hours if there is a justifiable reason, but even in such a case, the obligation itself is not exempted.

Is there a generally applicable obligation to notify the authorities of a data breach in your jurisdiction?

Under the PIPA, in the event of a data breach of a certain scale (i.e. a scale not smaller than the scale prescribed by the Presidential Decree), the personal information manager is required to report the fact of data breach and the results of the measures taken for such data breach to the Ministry of Government Administration and Home Affairs or a special agency designated by the Presidential Decree.

Under the Information and Communications Network Act, if an information and communications service provider becomes aware of a loss, theft or leak of personal information, the information and communications service provider is required to notify the relevant users of certain matters concerning such event (as prescribed by the Information and Communications Network Act), and to report to the Korea Communication Commission or the Korea Internet and Security

Agency. The notification and report, without any justifiable reason, must not be made after the lapse of 24 hours from the time when the communications service provider becomes aware of such event.

Are there sector specific mandatory data breach notification obligations in your jurisdiction?

Under the Credit Information Act, if a credit information company becomes aware of a leak of credit information for a purpose other than the intended business purposes, the credit information company must promptly notify the subject of the credit information of such leakage.

Bo-Seong Kim
Attorney at Law, Kim, Choi & Lim
02.721.4221
boskim@kcllaw.com

Junghwa Lee
Foreign Legal Advisor, Kim, Choi & Lim
02.721.4231
jhlee@kcllaw.com

TAIWAN

Is it unlawful in this jurisdiction to access third party data without authorisation? Is it unlawful to store data which has been accessed without authority?

Yes. The Personal Data Protection Act (PDPA) requires non public institutions to obtain the data subject's prior written well informed consent in order to collect, process or use personal data, and they must have a predefined purpose for collecting such data. In principle and subject to certain exceptions, non public institutions must (i) have a predefined purpose, and (ii) meet certain requirements prescribed by the law in order to process personal data.

Under the PDPA, public institutions may, but are not required to, obtain the data subject's consent when they act within the scope of their official responsibility or when there is no likelihood of injury to the data subject's rights and interests.

A public or non public institution that collects personal data must provide data subjects with information about the organisation's identity, the purposes for collecting personal data, third parties to which the organisation will disclose the personal data, the consequences of not providing consent, the rights of the data subject, how to make an inquiry or file a complaint, how to access/and or correct the data subject's personal data, and the duration of the proposed processing.

If an organisation is in violation of the PDPA, the competent authorities may take the following measures:

- Prohibit the organisation from collecting, processing or using personal information;
- Order the organisation to delete the personal information files already processed;
- Confiscate or order the organisation to destroy the personal information illegally collected; and
- Publicise the violation, the name of the non-compliant organisation and the name of the person in charge.

Is there a legal mechanism whereby you can seek access to or retrieve the copy of data which has been accessed without authority? Is there a legal mechanism that enables you find out information about who may have accessed your data without authority and/or how it was used?

Taiwan, a civil law jurisdiction, does not have common law pre trial procedures (including discovery). A victim of unauthorised use or access of personal data may initiate a lawsuit and request the court to investigate the relevant evidence (including information about who may have accessed the subject data without authority and/or how it was used) in the legal proceedings.

Is there any restriction on the use that can be made of the information or documentation obtained regarding a data breach incident using a legal process?

Rulings issued by Taiwan's Ministry of Justice (MOJ, the competent authority over the PDPA) provide that information procured/produced during legal proceedings can be used within the scope of performing legal duties and in compliance with the specific purpose of collection. Therefore:

- an attorney can use the transcript of a witness's testimony made in a criminal case in another civil litigation (No. Fa-Lv-Zi-10203510680 issued by the MOJ on October 14, 2013);
- the ID number of a debtor stated in a court judgment can be used in subsequent enforcement procedures (No. Yuan-Tai-Ting-Min-Yi-Zi-1030003167 issued by Judicial Yuan on January 29, 2014).

Is it possible to maintain confidentiality in relation to the legal steps necessary to get access to the data or information?

As mentioned above, Taiwan does not have common law pre-trial procedures (including discovery). For results of the relevant investigation conducted by the court, a party concerned may apply to the court clerk for inspection of, copying of, or photographing the investigation documents included in the dossier, or for a written copy, photocopy, or excerpted copy thereof with expenses advanced.

Where a third party files the above application with consent of the parties concerned, or with a preliminary showing of his/her legal interests concerned, the court may decide whether to grant approval for the application or not.

However, if the documents in the dossier involve the privacy or business secret of the party concerned or a third person and a grant of the application will likely result in material harm to such person, the court may, on motion or on its own initiative, render a ruling to deny the application or to restrict the acts outlined in the two preceding paragraphs.

If it is later determined that proceedings should be commenced in another jurisdiction (for example, the perpetrator is found to reside there), can you stop the proceedings in this jurisdiction in such a way that you are not prevented from commencing proceedings on the same issue as a result of the application of res judicata, double jeopardy or some other similar principle?

If proceedings are stopped because the court in Taiwan has no jurisdiction, the complainant will need to initiate another lawsuit in the appropriate jurisdiction and be prevented from commencing proceedings on the same issue in the court of Taiwan again. However, if proceedings are stopped

- not because the court in Taiwan lacks jurisdiction or because the plaintiff withdraws the suit;
- in a manner which does not result in a final determination of the issues in the proceedings; and
- with the consent of the other party concerned,

it will usually not prevent the plaintiff from commencing proceedings in this jurisdiction again. However, there may be an issue if proceedings are actively on foot in two jurisdictions at the same time which cover the same issues.

Is there an obligation in your jurisdiction to hold personal information securely?

Yes. Organisations are required to take steps to ensure that personal data in its possession and control is protected from unauthorised access and use, implement appropriate physical, technical and organisation security safeguards to protect personal data, and ensure that the level of security is in line with the amount, nature, and sensitivity of the personal data involved.

Under the PDPA, public institutions must designate personnel who are exclusively responsible for data protection. Non public institutions must take appropriate measures to prevent personal data from being stolen, amended, destroyed or disclosed.

Does the law in your jurisdiction restrict or place conditions on the transfer of personal or other information to other foreign jurisdictions?

Yes. Under the PDPA, the central competent authority may restrict international transmission of personal data by non public institutions in any of the following circumstances:

- Such transmission involves major national interest;
- Such transmission is subject to special provisions of an international treaty or agreement;
- The receiving country lacks proper laws and regulations that adequately protect personal data, and the rights and interests of a data subject are likely to be injured/damaged; or
- Personal data is indirectly transmitted to a third country (area) to evade the application of the PDPA.

Is there a generally applicable obligation to notify data subjects of a data breach in your Jurisdiction?

Yes. Under the PDPA, public institutions and non public institutions have the obligation to notify the affected individuals by appropriate means in the event of a data security breach. Under the Enforcement Rules for the PDPA, the "appropriate means" shall mean any method which can deliver the message to the affected individuals, including oral or written notice, telephone, facsimile, or electronic transmission. However, in the event that costs may be substantial, public notice is allowable. The notice should contain how the data security was breached and the remedy already adopted.

Is there a generally applicable obligation to notify the authorities of a data breach in your jurisdiction?

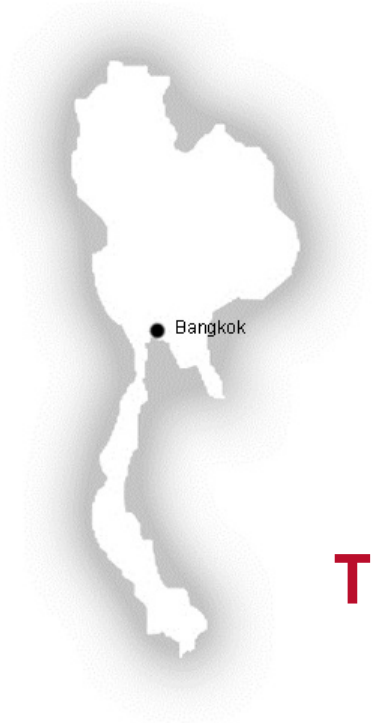
No. As of the date of this Guide, there is no generally applicable obligation to notify the authorities of a data breach under Taiwan law.

Are there sector specific mandatory data breach notification obligations in your jurisdiction?

Yes. According to the Regulations Governing the Personal Data Files Protection of the Non-public Institutions Designated by the Financial Supervisory Commission, in case of a material information security breach occurring in financial holding companies, banks, securities or futures enterprises, insurance companies, issuers of electronic stored value cards, other financial services providers designated by the Financial Supervisory Commission (FSC), and foundations supervised by the FSC, such entity shall notify the FSC of the information security breach.

As of the date of this Guide, the FSC is the only competent authority imposing the sector specific mandatory data breach notification obligations; however, there may be other competent authorities imposing such obligations in the future if they deem it necessary.

H. Henry Chang
Principal, Taipei
+88 6227157259
henry.chang@bakermckenzie.com



THAILAND

Is it unlawful in this jurisdiction to access third party data without authorisation? Is it unlawful to store data which has been accessed without authority?

It is illegal in Thailand to access third party computer data without authorisation according to the Act on Commission Offences Relating to Computer B.E. 2550 (2007) (the "Computer Crime Act") provided that there is a specific access prevention measure in place. The penalty is imprisonment and/or a fine.

The Thai government has recently initiated a digital economy plan in order to promote IT business and the digital environment in Thailand. One of the draft Bills under the digital economy plan is the Computer Crime Amendment Bill. There are certain revisions to the Computer Crime Act, e.g. if the computer data which is accessed without authorisation relates to national security, public security, national economic stability, or public service, the punishment is more severe. Nonetheless, as the Bill was recently approved in principle by the Cabinet in January 2015 and is currently under the consideration of the Council of State, it is subject to change. Therefore, it remains to be seen whether the Bill will be passed in this form.

Currently, there is no specific regulation prohibiting storing computer data which has been accessed without authority per se under the Computer Crime Act. Nonetheless, the storing of such data will be deemed as having in your possession an article which

has been obtained through illegal means. The data is then subject to search, seizure, and/or detention by the competent officials under court order. Please see further details of the legal search, seizure, and/or detention mechanism in the following section.

Is there a legal mechanism whereby you can seek access to or retrieve the copy of data which has been accessed without authority? Is there a legal mechanism that enables you find out information about who may have accessed your data without authority and/or how it was used?

If data owners can identify who accessed their data without authority and/or illegally, it is possible to apply for a search, seizure, and/or detention warrant under Thai law. However, there are criteria which must be met in order to apply for a search, seizure, and/or detention warrant. Nonetheless, the final decision rests with the court whether to grant a search, seizure, and/or detention warrant. Practically, there must be a strong prima facie case against the defendant(s) in order for the court to issue a search, seizure, and/or detention warrant.

For the benefit of an investigation, in the event that there is reasonable grounds to believe that there is perpetration of an offence under the Computer Crime Act, (e.g. unauthorised access of computer data with a specific access prevention measure in place), the competent official under the Act shall have certain authority, among others, only as necessary to identify the person who has committed the offence and/or how the data was used. For example, to inspect or access computer data which may be used as evidence on a necessity basis.

Is there any restriction on the use that can be made of the information or documentation obtained regarding a data breach incident using a legal process?

In the event that a data breach incident is identified and the applicant asks for an investigation to be conducted by the competent officials under the Computer Crime Act, there are certain restrictions on the use of the information or documentation obtained from the investigation. For example, the competent officials are obliged by the law not to disclose or deliver to others the computer data, computer traffic data or data of the users acquired under the investigation.

Is it possible to maintain confidentiality in relation to the legal steps necessary to get access to the data or information?

The investigation and gathering of evidence by the competent officials under the Computer Crime Act, (e.g. getting access to the data or confidential information), is generally confidential. There is no public statement announcing such

investigations. The competent officials are also obliged by the law not to disclose or deliver to others the computer data, computer traffic data or data of the users acquired under the investigation. Also, if any person happens to obtain such data from the relevant competent official, he/she is prohibited by law from disclosing such data to others.

If it is later determined that proceedings should be commenced in another jurisdiction (for example, the perpetrator is found to reside there), can you stop the proceedings in this jurisdiction in such a way that you are not prevented from commencing proceedings on the same issue as a result of the application of res judicata, double jeopardy or some other similar principle?

It is possible to stop the proceedings in Thailand on the basis that the proceedings are not yet final. This will not prevent the plaintiff from commencing proceedings on the same issue in another jurisdiction. Nonetheless, it will also depend on the law of that other jurisdiction whether the case which has already been conducted in Thailand, even though it is not yet final, will be able to be tried again in that jurisdiction.

Is there an obligation in your jurisdiction to hold personal information securely?

Yes. There are certain security regulations and obligations in Thailand to protect personal information from misuse, interference and loss and from unauthorised access, modification and disclosure. For example, telecommunication operators must provide security measures for personal information both technically and provide security within the organisation of the telecommunications operators. Also, the levels of security measure obligations are more stringent if such personal information is sensitive, e.g. certain personal information as provided in banking and financial institution regulations.

Does the law in your jurisdiction restrict or place conditions on the transfer of personal or other information to other foreign jurisdictions?

Yes. There are certain sector specific regulations restricting the transfer of information overseas. For example, the credit bureau is prohibited from transferring credit data to foreign jurisdictions.

Also, the Personal Data Protection Bill, which was one of the Bills approved in principle by the Cabinet in January 2015 under the government's digital economy plan, specifies certain restrictions on the transfer of personal data overseas. That is, the transfer shall be in accordance with the rules prescribed by the Personal

Data Protection Committee regarding the protection of personal data sent or transferred abroad, unless certain exceptions apply. Nonetheless, as the Bill is currently under the consideration of the Council of State, it is subject to change. Therefore, it remains to be seen whether the Bill will be passed in this form.

Is there a generally applicable obligation to notify data subjects of a data breach in your Jurisdiction?

While there is currently no consolidated general data protection law to require notifying the data subject of data breach in Thailand, there are certain sector specific regulations imposing such obligations. For example, telecommunications operators must notify data subjects of the breach without delay.

Also, the Personal Data Protection Bill contains an obligation to notify data subjects immediately of any breach of personal data and the remedial plan for the damage arising from such breach of personal data. Again, as the Bill is currently under the consideration of the Council of State, it is subject to change. Therefore, it remains to be seen whether the Bill will be passed in this form.

Is there a generally applicable obligation to notify the authorities of a data breach in your jurisdiction?

While there is currently no consolidated general data protection law to require notifying the authorities of a data breach in Thailand, the Personal Data Protection Bill contains an obligation to notify the Personal Data Protection Committee of certain details of such a breach, in the event that the breach affects people in a number exceeding that as prescribed by the Personal Data Protection Committee. Nonetheless, it remains to be seen whether the Bill will be passed in this form.

Are there sector specific mandatory data breach notification obligations in your jurisdiction?

Yes. As mentioned above, there are certain sector specific mandatory data breach notification obligations in Thailand in connection with electronic payment service providers, telecommunications operators, and the credit bureau.

Dhiraphol Suwanprateep
Partner, Bangkok
+66 2636 2000
dhiraphol.suwanprateep@bakermckenzie.com

VIETNAM

Is it unlawful in this jurisdiction to access third party data without authorisation? Is it unlawful to store data which has been accessed without authority?

Yes. Using passwords or information of organisations or individuals without their authorisation is prohibited.[4] Stealing, using, revealing, transferring or selling information relating to the business secrets of other traders, organisations or individuals, or the personal information of consumers in e-commerce, without the consent of the parties concerned, is unlawful.[5]

Generally, the collection and publication of information and materials that constitute an individual's personal information must be consented to by that person. In cases where that person has died, lost his/her capacity or is under 15 years, the consent of his/her family member or representative is required, except for cases where the collection and publication of information and materials are made by the decision of a competent agency or organisation.[6]

Personal information may be collected, processed, and used without consent in the following cases:

- Concluding, modifying or performing contracts on the use of information, products or services in the network environment;

4 Article 5.4 Decree No. 72/2013/ND-CP.

5 Article 4.4.a Decree No. 52/2013/ND-CP.

6 Article 38.2 Civil Code No. 33/2005/QH11 ("Civil Code").

- Calculating charges for use of information, products or services in the network environment;
- Performing other obligations provided for by law.[7]

Is there a legal mechanism whereby you can seek access to or retrieve the copy of data which has been accessed without authority? Is there a legal mechanism that enables you find out information about who may have accessed your data without authority and/or how it was used?

No. There is no legal mechanism for such purpose.

Generally, competent authorities can request that entities provide information and materials if needed.[8] In case a data breach is considered a cybercrime, competent authorities are allowed to seek access to or retrieve a copy of data that has been accessed without authority as well as find out the person who accessed the data without authority.[9] However, this is not available as a legal mechanism for the data subjects/data owners.

Is there any restriction on the use that can be made of the information or documentation obtained regarding a data breach incident using a legal process?

No. There is no specific regulation on this issue.

Is it possible to maintain confidentiality in relation to the legal steps necessary to get access to the data or information?

There is no specific regulation on this issue.

If it is later determined that proceedings should be commenced in another jurisdiction (for example, the perpetrator is found to reside there), can you stop the proceedings in this jurisdiction in such a way that you are not prevented from commencing proceedings on the same issue as a result of the application of res judicata, double jeopardy or some other similar principle?

Generally it is possible to suspend, rather than withdraw, the petition for any civil action in Vietnamese courts without prejudice.

7 Articles 21.3 Law No. 67/2006/QH11 on Information Technology ("Law on Information Technology").

8 Article 38.2 Civil Code; Article 14.3 Law No. 47/2010/QH12 on Credit Institutions ("Law on Credit Institutions").

9 Article 14.1 Decree No. 25/2014/ND-CP.

Is there an obligation in your jurisdiction to hold personal information securely?

Yes. Generally, letters, telephones, telegrams, and other forms of electronic information of individuals shall be safely and confidentially guaranteed.[10]

Organisations and individuals that collect, process and use personal information of other people have to take necessary managerial and technical measures to ensure that personal information shall not be lost, stolen, disclosed, modified or destroyed.[11]

In transactions with consumers, consumers' information shall be kept safe and confidential when they participate in transactions or use goods or services, except where competent state agencies require the information.[12]

In electronic transactions, agencies, organisations and individuals must not use, provide or disclose information on private and personal affairs or information of other agencies, organisations and/or individuals which is accessible by them or under their control in e-transactions without the latter's consent, unless otherwise provided for by law.[13] Agencies, organisations and individuals conducting e-transactions must take necessary measures to ensure smooth operations of information systems under their control. If they cause technical errors to such information systems which cause damage to other agencies, organisations and/or individuals, they shall be handled in accordance with the provisions of the law.[14]

Specifically, e-commerce data collectors must ensure that personal information which they have collected and stored is safe and secure and must prevent the following acts:

- Hacking or illegally accessing information;
- Illegally using information;
- Illegally altering or destroying information.[15]

10 Article 38.3 Civil Code.

11 Article 21.1.c Law on Information Technology.

12 Article 6.1 Law No. 59/2010/QH12 on Protection of Consumers' Rights ("Law on Protection of Consumers' Rights").

13 Article 46.2 Law No. 51/2005/QH11 on Electronic Transactions ("Law on Electronic Transactions").

14 Article 44.2 Law on Electronic Transactions.

15 Article 72.1 Decree No. 52/2013/ND-CP.

Does the law in your jurisdiction restrict or place conditions on the transfer of personal or other information to other foreign jurisdictions?

No. Generally, there is no restriction or condition on the transfer of personal or other information from Vietnam to other foreign jurisdictions provided the requisite consent of the data subjects has been obtained.

Is there a generally applicable obligation to notify data subjects of a data breach in your Jurisdiction?

No. There is no specific obligation to notify data subjects of a data breach in Vietnam.

Is there a generally applicable obligation to notify the authorities of a data breach in your jurisdiction?

Yes. Generally, providers and users of internet services and online information are responsible for ensuring information safety and information security within their information system and cooperating with competent authorities, other organisations and individuals in ensuring online information safety and information security.[16] Cooperating with competent authorities can be interpreted to include notifying the authorities of a data breach.

Are there sector specific mandatory data breach notification obligations in your jurisdiction?

Yes. In the e-commerce sector, if an information system is hacked, posing a risk of loss of consumer information, information storing units shall notify the incident to a functional agency within twenty-four hours after detecting it.[17]

Yee Chung Seck
Partner, Ho Chi Minh City
+84 8 3520 2633
yeechung.seck@bakermckenzie.com

16 Article 28.1 Decree No. 72/2013/ND-CP.

17 Article 72.3 Decree No. 52/2013/ND-CP.

Baker & McKenzie Asia Pacific Offices

Office phone numbers and addresses change from time to time. Please refer to www.bakermckenzie.com for current contact information.

Australia - Melbourne
Baker & McKenzie
Level 19
181 William Street
Melbourne VIC 3000
Australia
Tel: +61 3 9617 4200
Fax: +61 3 9614 2103

Australia - Brisbane
Baker & McKenzie
Level 8
175 Eagle Street
Brisbane QLD 4000
Australia
Tel: +61 7 3069 6200
Fax: +61 7 3069 6201

Australia - Sydney
Baker & McKenzie
Level 27, AMP Centre
50 Bridge Street
Sydney, NSW 2000
Australia
Tel: +61 2 9225 0200
Fax: +61 2 9225 1595

China - Beijing
Baker & McKenzie LLP - Beijing
Representative Office
Suite 3401, China World Office 2
China World Trade Center
1 Jianguomenwai Dajie
Beijing 100004, PRC
China
Tel: +86 10 6535 3800
Fax: +86 10 6505 2309

China - Hong Kong - SAR
Baker & McKenzie
Hutchison House
14th Floor, Hutchison House
10 Harcourt Road, Central
Hong Kong SAR

and

23rd Floor, One Pacific Place
88 Queensway
Hong Kong SAR
China
Tel: +852 2846 1888
Fax: +852 2845 0476

China - Shanghai
Baker & McKenzie LLP
Unit 1601, Jin Mao Tower
88 Century Avenue, Pudong
Shanghai 200121, PRC
China
Tel: +86 21 6105 8558
Fax: +86 21 5047 0020

Indonesia - Jakarta
Hadiputranto, Hadinoto & Partners
The Indonesia Stock Exchange Building
Tower II, 21st Floor
Sudirman Central Business District
Jl. Jendral Sudirman Kav. 52-53
Jakarta 12190
Indonesia
Tel: +62 21 2960 8888
Fax: +62 21 2960 8999

Japan - Tokyo
Baker & McKenzie
(Gaikokuho Joint Enterprise)
Ark Hills Sengokuyama Mori Tower, 28th Floor
1-9-10 Roppongi, Minato-ku
Tokyo 106-0032
Japan
Tel: +81 3 6271 9900
Fax: +81 3 5549 7720

Malaysia - Kuala Lumpur
Wong & Partners
Level 21, The Gardens South Tower
Mid Valley City
Lingkaran Syed Putra
Kuala Lumpur 59200
Malaysia
Tel: +603 2298 7888
Fax: +603 2282 2669

Myanmar - Yangon
Baker & McKenzie Yangon
1203 12th Floor Sakura Tower
339 Bogyoke Aung San Road
Kyauktada Township
Yangon
Myanmar
Tel: +95 1 255 056
Fax: +95 1 255 057

Philippines - Manila
Quisumbing Torres
12th Floor, Net One Center
26th Street Corner 3rd Avenue
Crescent Park West
Bonifacio Global City
Taguig City 1634
Philippines
Tel: +63 2 819 4700
Fax: +63 2 816 0080

Singapore
Baker & McKenzie.Wong & Leow
8 Marina Boulevard
#05-01 Marina Bay Financial Centre
Tower 1
Singapore 018981
Tel: +65 6338 1888
Fax: +65 6337 5100

South Korea - Seoul
Foreign Legal Consultant Office
17/F, Two IFC
10 Gukjegeumyung-ro
Yeongdeungpo-gu
Seoul 150-945
South Korea
T +82 2 6137 6800
F +82 2 6137 9433

Taiwan - Taipei
Baker & McKenzie
15/F, 168 Tun Hwa North Road
Taipei 105,
Taiwan
Tel: +886 2 2712 6151
Fax: +886 2 2712 8292

Thailand - Bangkok
Baker & McKenzie Limited
25th Floor, Abdulrahim Place
990 Rama IV Road
Bangkok 10500
Thailand
Tel: +66 2636 2000
Fax: +66 2636 2111

Vietnam - Hanoi
Baker & McKenzie (Vietnam) Ltd.
(Hanoi Branch Office)
Unit 1001, 10th floor,
Indochina Plaza Hanoi
241 Xuan Thuy Street, Cau Giay District
Hanoi 10000
Vietnam
Tel: +84 4 3825 1428
Fax: +84 4 3825 1432

Vietnam - Ho Chi Minh City
Baker & McKenzie (Vietnam) Ltd. (HCMC)
12th Floor, Saigon Tower
29 Le Duan Blvd.
District 1
Ho Chi Minh City
Vietnam
Tel: +84 8 3829 5585
Fax: +84 8 3829 5618

www.bakermckenzie.com

Baker & McKenzie has been global since our inception. It is part of our DNA.

Our difference is the way we think, work and behave – we combine an instinctively global perspective with a genuinely multicultural approach, enabled by collaborative relationships and yielding practical, innovative advice. With 5,300 lawyers in 47 countries, we have a deep understanding of the culture of business the world over and are able to bring the talent and experience needed to navigate complexity across practices and borders with ease.