Recent Developments of Hong Kong Personal Data Privacy Protection

Mr Stephen Wong
Privacy Commissioner for Personal Data, Hong Kong

Personal Data Privacy Protection

- 1996 Personal Data (Privacy) Ordinance (Cap 486) – "to protect the privacy of individuals in relation to personal data"; "to safeguard free flow of personal data to HK"

- Strike a balance between personal data privacy and the free flow of information/ free expression is one of our important tasks and missions.
- Maintain and develop HK as an international centre for communication.

Personal Data Privacy Protection Landscape

Sweden
(1973)

109 Jurisdictions
(Feb 2015)

Recent Developments –

I. Personal Data Protection in Cross Border Data Transfer

Section 33 of the Personal Data (Privacy) Ordinance

- Section 33 of the PDPO prohibits transfer of personal data outside Hong Kong unless under specified circumstances (this provision is not yet operative)

- Intent: to ensure that the personal data transferred outside Hong Kong will be afforded with comparable protection under the PDPO

- Restriction on cross border data flow is commonly found in the data protection laws in other jurisdictions.

Overseas Cross-border Transfer Restriction

Jurisdictions	Cross-border transfer restriction	In force
European Union	European Union Directive 95/46/EC, Art. 25	✓
United Kingdom	Data Protection Act 1998, DPP 8	✓
Australia	Privacy Act 1988, APP 8	✓
New Zealand	Privacy Act 1993, Part 11A	✓
Singapore	Personal Data Protection Act 2012, section 26 Part VI	✓

Meaning of Transfer

- s.33 covers two situations:

(i) Transfer of personal data from Hong Kong to a place outside Hong Kong

(ii) Transfer of personal data between two other jurisdictions where the transfer is controlled by a data user in Hong Kong

- No definition of "transfer" under the PDPO
- Ordinary meaning applies: transmission from one place or person to another (≠ mere transit) (e.g. sending paper or electronic documents containing personal data by courier, post or electronic means)

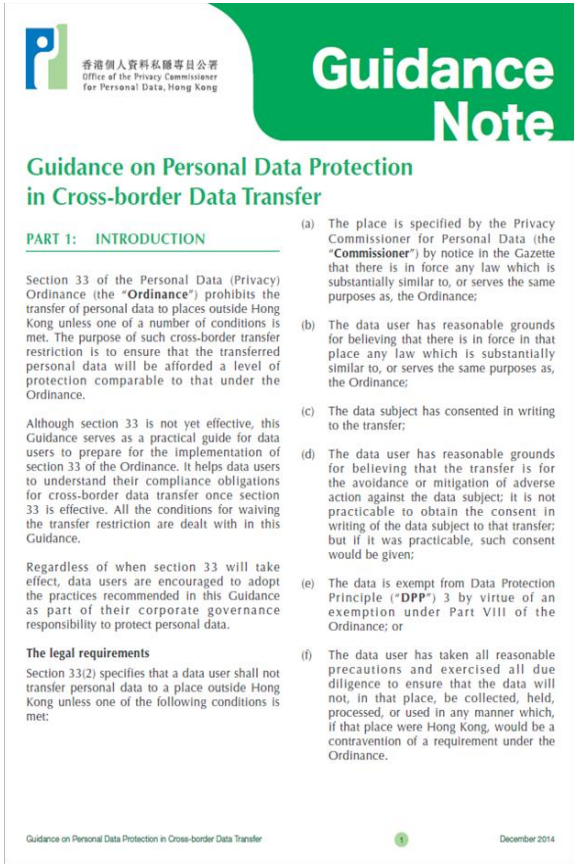
Section 33 of the Personal Data (Privacy) Ordinance

- The PCPD had undertaken the necessary preparatory work including a 'white list' of jurisdictions with privacy standards comparable to that of Hong Kong; and published a Guidance Note on Personal Data Protection in Cross-border Data Transfer in Dec 2014.

- Guidance: voluntary compliance; adopt as part of corporate governance responsibility to protect personal data (before implementation).

- Served as starting point for the Government's determination of the next step.

- The PCPD currently assists the Government and its consultant by providing advice on the issues arising from the Guidance and the topic.



香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

Guidance Note

Guidance on Personal Data Protection in Cross-border Data Transfer

PART 1: INTRODUCTION

Section 33 of the Personal Data (Privacy) Ordinance (the "**Ordinance**") prohibits the transfer of personal data to places outside Hong Kong unless one of a number of conditions is met. The purpose of such cross-border transfer restriction is to ensure that the transferred personal data will be afforded a level of protection comparable to that under the Ordinance.

Although section 33 is not yet effective, this Guidance serves as a practical guide for data users to prepare for the implementation of section 33 of the Ordinance. It helps data users to understand their compliance obligations for cross-border data transfer once section 33 is effective. All the conditions for waiving the transfer restriction are dealt with in this Guidance.

Regardless of when section 33 will take effect, data users are encouraged to adopt the practices recommended in this Guidance as part of their corporate governance responsibility to protect personal data.

The legal requirements

Section 33(2) specifies that a data user shall not transfer personal data to a place outside Hong Kong unless one of the following conditions is met:

(a) The place is specified by the Privacy Commissioner for Personal Data (the "**Commissioner**") by notice in the Gazette that there is in force any law which is substantially similar to, or serves the same purposes as, the Ordinance;

(b) The data user has reasonable grounds for believing that there is in force in that place any law which is substantially similar to, or serves the same purposes as, the Ordinance;

(c) The data subject has consented in writing to the transfer;

(d) The data user has reasonable grounds for believing that the transfer is for the avoidance or mitigation of adverse action against the data subject; it is not practicable to obtain the consent in writing of the data subject to that transfer; but if it was practicable, such consent would be given;

(e) The data is exempt from Data Protection Principle ("**DPP**") 3 by virtue of an exemption under Part VIII of the Ordinance; or

(f) The data user has taken all reasonable precautions and exercised all due diligence to ensure that the data will not, in that place, be collected, held, processed, or used in any manner which, if that place were Hong Kong, would be a contravention of a requirement under the Ordinance.

Guidance on Personal Data Protection in Cross-border Data Transfer 1 December 2014

CJEU's decision concerning 'Safe Harbour'

Background

- This Court of Justice of the European Union ("CJEU") case was a referral from the Irish High Court, based on a claim by Max Schrems that Facebook was involved in large-scale data collection by US intelligence, and that Facebook was in breach of EU-US data transfer rules when it transferred users' data from Ireland to the US.
- The Irish Data Protection Authority rejected Schrems' complaint, citing that it was bound by the now-impugned EU's Decision (in 2000) (on adequacy of the "Safe Harbour"). Schrems brought the case to the Irish High Court, which referred it to the CJEU.

CJEU's decision concerning 'Safe Harbour'

The CJEU handed down (6 Oct 2015) a decision which carries the following meaning:

- The decision – that the 'safe harbour' programme for data transfer between US and EU provided "adequate protection" under EU privacy laws – was invalid.
- In other words, operating within the 'safe harbour' framework is, by itself, no longer sufficient to satisfy the "adequacy requirement" under the EU Directive for data transfer from EU to the US.
- National data protection authorities ("DPAs") still have the power to independently review whether a cross-border transfer of personal data in each case complies with the EU Directive.

CJEU's decision concerning 'Safe Harbour'

A statement issued by The EU Article 29 Working Party (WP29) (16 Oct 2015) :

- Data transfers from EU to the US can no longer be framed solely on the basis of the EU Decision (on 'safe harbour' adequacy).

- There is an urgent need to open negotiations with US authorities to find a solution to enable data transfer, e.g. by an intergovernmental agreement providing stronger guarantees to EU data subjects.

CJEU's decision concerning 'Safe Harbour'

- By the end of January 2016, if no appropriate solution is found with the US authorities, EU DPAs will take action, which may include coordinated enforcement action.

- Standard Contractual Clauses and Binding Corporate Rules can still be used as a basis for EU-US data transfers, in the meantime.

CJEU's decision concerning 'Safe Harbour'

- The **US *Judicial Redress Bill*** would allow some foreigners the right to pursue their privacy rights in US courts. The Bill is now pending adoption by the Senate.

- The Bill seeks to extend some of the rights that US citizens currently enjoy also to Europeans. Therefore it will increase the level of data protection for EU data subjects, and address some of the key problems and facilitate negotiations over a new data transfer regime.

Implications of CJEU ruling on Protection of Cross-Border Data Transfer in Hong Kong

- It adds uncertainty to the steps that should be taken to ensure comparable protection for data transfer to the US

- Organisations should take other measures such as entering into contracts with the recipient organisations to ensure adequate level of protection to be afforded to the personal data transferred overseas.

Implications of CJEU ruling on Protection of Cross-Border Data Transfer in Hong Kong

- The HKSAR Government has engaged a consultant to conduct a business impact assessment for implementation of section 33. The effect of the CJEU's ruling would have to be taken into consideration when making an overall assessment.

- Ultimately a balance would need to be struck between achieving the underlying purpose of the provision and avoiding adverse impact on businesses.

Recent Developments –

II. The Right to be Forgotten and David Webb case

The Right to be Forgotten

The Court of Justice of the European Union (CJEU) decision in Google Spain widely reported as a "Right to be forgotten" case.

- The CJEU ruled that, an individual has the right to request search engines to **de-list search results** which link his personal name to certain online publications, for searches performed using his name.

- This applies where the information is **"inadequate, irrelevant or no longer relevant, or excessive"** for the purpose of the data processing and in the light of the time that has elapsed since the original publication.

The Right to be Forgotten

- The CJEU decision is concerned with **striking a balance between an individual's personal data privacy, and the public interest** in accessing information**.**

- The court ruled that a **case-by-case assessment** is needed to consider the type of information in question, its sensitivity for the individual's private life and the interest of the public in having access to that information, taking into consideration the public role the individual may hold.

- EU Guidelines (by Article 29 Data Protection Working Party) articulated 13 criteria when deciding whether a request to de-list information should be accepted.

The Right to be Forgotten is not absolute

- The "right to be forgotten", though a convenient label, is a misnomer as no published material is required to be deleted through exercise of the right. It empowers individuals to control the online dissemination of information about them and involves the de-listing of Internet search results.

- The original information continues to exist at the source and can be accessed online directly or by search using other search terms (as in the case of the CJEU where the court ruled against Google requiring it to delink, while upholding the right of the newspaper to retain the original notice).

PCPD's view

- The "right to be forgotten" is still a very fluid concept and rapid developments are expected.

- The PCPD will continue to monitor the development. We are **NOT** promoting privacy as an absolute right. We have to **seek a balance between privacy and other rights and interests,** incl. freedom of expression and of the press. These rights are of equal value in a civil society and none has pre-eminence over others.

David Webb Case = the Right to be Forgotten?

Administrative Appeals Board's Decision on Dismissing David Webb's Appeal Case

Background:

- The Complainant and her ex-husband were parties to the matrimonial appeal heard in Court of Appeal, of which three judgments were handed down in 2000, 2001 and 2002. Pursuant to an internal direction from Chief Justice, with effect from April 2011 **all judgments in family and matrimonial cases** at every level of courts, whether in open court or in chambers, should be anonymised before release.

- This policy is consistent with Article 10 of the Hong Kong Bill of Rights which excludes judgments of proceedings concerning matrimonial disputes from being made public.

Administrative Appeals Board's Decision on Dismissing David Webb's Appeal Case

Background:

- At the request of the Complainant, in 2010 the Judiciary replaced her name by an alphabet in these three judgments. However, later the Complainant found her name listed alongside the three hyperlinks on "Who's Who" of a website named "Webb-site" established by Mr Webb. The hyperlinks were respectively connected to the three anonymised judgments in the Legal Reference System of the Judiciary's website.
- The Complainant was aggrieved that through Webb-site, Mr Webb has revealed her identity in the three anonymised judgments by the hyperlinks, and hence lodged a complaint with PCPD.

Administrative Appeals Board's Decision on Dismissing David Webb's Appeal Case

- PCPD concluded that **Mr Webb had contravened the Data Protection Principle 3 ("DPP 3") of the Ordinance by publishing the hyperlinks on Webb-site which effectively disclosed the Complainant's identity in the three anonymised judgments.**

- On 26 August 2014, PCPD served upon Mr Webb the Result of Investigation and Enforcement Notice directing him to remove the three hyperlinks from Webb-site. He subsequently lodged an appeal against PCPD's decision.

David Webb Case = the Right to be Forgotten?

- The AAB's recent decision has confirmed the PCPD's determination which is focused on the disclosure of the Complainant's name by the 'Webb-site', in contravention of DPP3.

- The AAB did not find that Webb's purpose of using the complainant's name (i.e. publication for general reporting) to be consistent with the judiciary purposes of publishing the judgements (i.e. to enable them to be used as "legal precedents on points of law, practices and procedure of the Courts and of public interest").

David Webb Case = the Right to be Forgotten?

- David Webb case was largely based on the particular factual circumstances of the case, and should be distinguished from the Google Spain decision on the right to be forgotten.

- The peculiar circumstance of the David Webb case relates to the nature of the original published articles (i.e. the court judgments) which themselves have been anonymised based on the Chief Justice's direction. [vs. the information (without redaction) in its origins in Google Spain case can still be traced].

David Webb Case = the Right to be Forgotten?

- The decision has no adverse impact on the public's right to access information. It does not affect information reported by or stored on news websites or news archives. That information can remain in their original form (i.e. bearing the data subjects' names) for retention and distribution.

- In weighing the freedom of press and expression against the personal data privacy of the Complainant, the PCPD was of the view that the disclosure of the Complainant's identity in the three anonymized matrimonial judgments did not serve to promote the transparency of operations of companies, governments, regulators and controlling shareholders; nor was it able to achieve the purpose of condemning public vices or protecting the minority shareholders' interest.

David Webb Case = the Right to be Forgotten?

- *"Unfortunately, contrary to David Webb's assertion, this certainly does NOT establish a 'right to be forgotten' or even a 'right to be rehabilitated' which is a more accurate description of what the ECJ established."*

- *"The major problem is that this 'right' has been wrongly framed."... "I believe that most reasonable individuals believe that rehabilitation is important, not only for minors, but, at least for minor mistakes/offences, for adults as well."*

Professor John Bacon-Shone

Associate Dean (Knowledge Exchange),Faculty of Social Sciences,

The University of Hong Kong

Recent Developments –

III. Privacy Management Programme

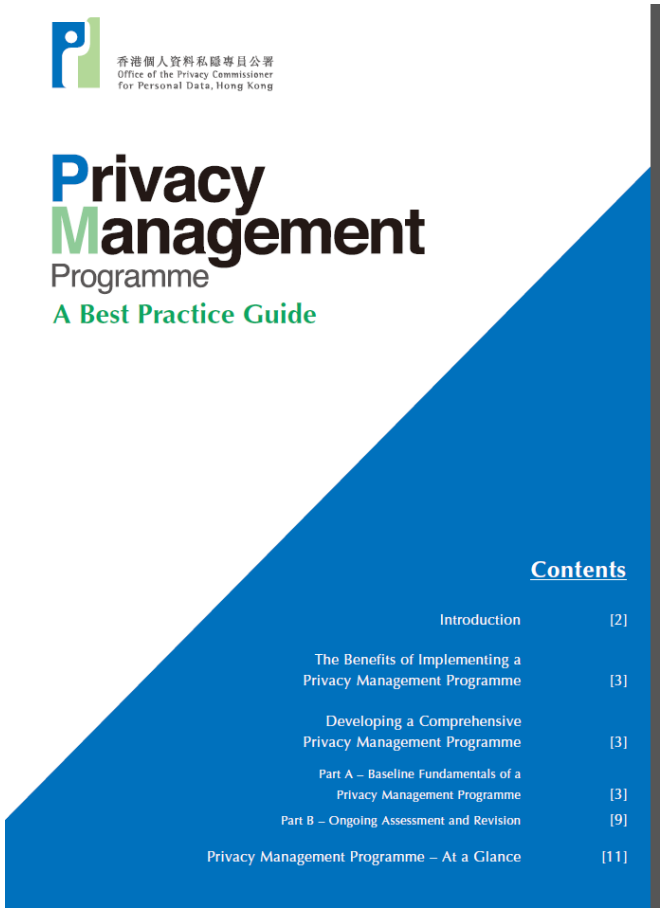
Advocating Privacy Protection as Corporate Governance

- PCPD advocates that organisations should make personal data protection part of their corporate governance responsibilities. The maintenance of a comprehensive privacy management programme ("PMP") is of paramount importance.

- In February 2014, the Hong Kong SAR Government, together with 25 companies from the insurance sector, 9 companies from the telecommunications sector and 5 organisations from other sectors, all pledged to implement PMP.

From Compliance to Accountability

- PCPD released a PMP: A Best Practice Guide in February 2014. The Guide outlines the building blocks of PMP, a strategic framework to protect personal data privacy. It provides insight and guidance to organisations when they develop and improve their own programmes according to their specific circumstances, such as organisation size, nature of business, and the amount and sensitivity of the personal data they collect and manage.



Accountability Benchmarking Micro-Study

In collaboration with Nymity, PCPD conducted the Hong Kong Accountability Benchmarking Micro-Study in 2015. The results showed that:

- Hong Kong organisations have made significant strides in embracing data protection as part of their corporate governance responsibilities, shifting from compliance to accountability.

- Many organisations in Hong Kong are taking privacy seriously and the subject is now on the agenda of their top management.

- A higher percentage of organisations in Hong Kong implement personal data inventory and data classification compared with other global organisations.

Accountability Benchmarking Micro-Study (Cont'd)

Key findings of the benchmarking analysis report include:

• As a priority, participating organisations have implemented activities that focus on legal compliance requirements and a specific Code of Practice (HR Management) issued by PCPD;

• Participating organisations have invested heavily in privacy and data protection measure related to technical and security measures, records retention, data privacy notices and policies, requirements for processors, and managing and responding to access requests ;

• Participating organisations have indicated their endeavour to further develop the PMP in the following areas: training and awareness; managing third-party risk; access requests, inquiries and complaints; expanding PIA programs and implementing privacy by design procedures; and, testing incident and breach protocols .

Consultancy Project on PMP in 2016

PCPD is collaborating with the HKSAR Government to assist 3 bureaux / departments to develop or review their respective PMPs through consultancy services.

- The objectives of the consultancy project are to design and implement tailor-made PMPs, or review and revise existing PMPs for the selected bureaux / departments to be used as model cases and to transfer the knowledge and experience gained from the model cases to other bureaux / departments.

- The consultancy project will bring in the special knowledge and expertise of the consultant which are currently not available internally. Through these efforts, we would spearhead changes in realising the best practice of PMP in the 3 government bureaux / departments and facilitate further adoption of the same in other bureaux / departments.

Recent Developments –

IV. Direct marketing regulatory regime in Hong Kong

More Stringent Requirements

- The regulatory regime for direct marketing activities under the Ordinance has been substantially revamped and come into force on 1 April 2013.

- It is an offence if organisations do not take specified action to notify individual consumers and obtain their consent before using the personal data in direct marketing. Failure to comply with this will attract a fine up to HK$500,000 and imprisonment for up to 3 years.

- If the data is provided to a third party for its use in direct marketing in exchange for gain, non-compliance may result in a maximum penalty of a fine of HK$1 million and 5 years' imprisonment.

Enforcements

- PCPD has been working closely with DoJ and Police

- Since the amended Ordinance came into force (and up to 30 September 2015), the PCPD has received 9,299 enquiries and 984 complaints in relation to direct marketing.

- Among these complaints, 45 cases were referred to Police for criminal investigation, and of which 5 cases had been prosecuted. Three of them were concluded in convictions while the remaining 2 are awaiting trials.

Conviction of Offence
Relating to Use of Personal Data in Direct Marketing

1st Convicted Case - An Internet Service Provider (September 2015)	**Failure to comply with customer's opt-out request (i.e. cease to use his personal data in direct marketing)**	**Fined HK$30,000**
2nd Convicted Case – A Storage Service Provider (September 2015)	Using the personal data of a customer in direct marketing without taking specified actions	Fined HK$10,000
3rd Convicted Case – A Body Check Service Company (November 2015)	Failure to comply with customer's opt out request	Fined HK$10,000

Strengthen the Culture of Respecting Personal Data Privacy

- The successful conviction will serve as a deterrent and convey a strong message to organisations engaging in direct marketing activities that consumers' personal data must be respected.

- Companies should conduct direct marketing activities in a more customer-focused manner in order to build customer trust, and enhance the professionalism of the industry.

- Building a culture to protect and respect personal data in companies become important.

PCPD.org.hk

保障、尊重個人資料

Protect, Respect Personal Data

Important

The contents herein are for general reference only. It does not provide an exhaustive guide to the application of the Personal Data (Privacy) Ordinance ("the Ordinance"). For a complete and definitive statement of law, direct reference should be made to the Ordinance itself. The Privacy Commissioner for Personal Data ("the Commissioner") makes no express or implied warranties of accuracy or fitness for a particular purpose or use with respect to the above information. The contents herein will not affect the exercise of the functions and power conferred to the Commissioner under the Ordinance.

Thank you

Office of the Privacy Commissioner for Personal Data, Hong Kong

- Enquiry Hotline: (852) 2827 2827
- Fax : (852) 2877 7026
- Website : www.pcpd.org.hk
- Email : enquiry@pcpd.org.hk
- Address : 12/F, Sunlight Tower, 248 Queen's Road East Wanchai, Hong Kong