The University of Hong Kong

Road to Data Privacy and Protection in Direct Marketing Activities

16-Nov-2017
Data privacy breaches do happen….
Who will be the next target?

<table>
<thead>
<tr>
<th>Year</th>
<th>No. of Complaints in HK</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>1995</td>
<td>10</td>
<td>Enactment of PDPO</td>
</tr>
<tr>
<td>1996</td>
<td>227</td>
<td>Magazine case</td>
</tr>
<tr>
<td>1997</td>
<td>392</td>
<td>Hong Kong search engine case</td>
</tr>
<tr>
<td>1998</td>
<td>541</td>
<td>Consultation paper</td>
</tr>
<tr>
<td>1999</td>
<td>692</td>
<td>Enactment of Personal Data (Privacy) (Amendment) Ordinance 2012</td>
</tr>
<tr>
<td>2000</td>
<td>843</td>
<td>Contactless smart card operator case</td>
</tr>
<tr>
<td>2001</td>
<td>921</td>
<td>Government authority in healthcare case</td>
</tr>
<tr>
<td>2002</td>
<td>984</td>
<td>Contactless smart card operator case</td>
</tr>
<tr>
<td>2003</td>
<td>900</td>
<td>Contactless smart card operator case</td>
</tr>
<tr>
<td>2004</td>
<td>989</td>
<td>Contactless smart card operator case</td>
</tr>
<tr>
<td>2005</td>
<td>1025</td>
<td>Contactless smart card operator case</td>
</tr>
<tr>
<td>2006</td>
<td>937</td>
<td>Contactless smart card operator case</td>
</tr>
<tr>
<td>2007</td>
<td>1179</td>
<td>Contactless smart card operator case</td>
</tr>
<tr>
<td>2008</td>
<td>1213</td>
<td>Contactless smart card operator case</td>
</tr>
<tr>
<td>2009</td>
<td>1486</td>
<td>Contactless smart card operator case</td>
</tr>
<tr>
<td>2010</td>
<td>1792</td>
<td>Contactless smart card operator case</td>
</tr>
<tr>
<td>2011</td>
<td>1702</td>
<td>Contactless smart card operator case</td>
</tr>
<tr>
<td>2012</td>
<td>838</td>
<td>Contactless smart card operator case</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Year</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>1997</td>
<td>Commencement of provisions on direct marketing activities</td>
</tr>
<tr>
<td>1998</td>
<td>Fitness centre case</td>
</tr>
<tr>
<td>1999</td>
<td>Government authority in healthcare case</td>
</tr>
<tr>
<td>2000</td>
<td>Monitoring and Personal Data Privacy at Work</td>
</tr>
<tr>
<td>2001</td>
<td>Travel Agent Membership Program</td>
</tr>
<tr>
<td>2002</td>
<td>Consultation paper</td>
</tr>
<tr>
<td>2003</td>
<td>Enactment of Personal Data (Privacy) (Amendment) Ordinance 2012</td>
</tr>
<tr>
<td>2004</td>
<td>Contactless smart card operator case</td>
</tr>
<tr>
<td>2005</td>
<td>Contactless smart card operator case</td>
</tr>
<tr>
<td>2006</td>
<td>Contactless smart card operator case</td>
</tr>
<tr>
<td>2007</td>
<td>Contactless smart card operator case</td>
</tr>
<tr>
<td>2008</td>
<td>Contactless smart card operator case</td>
</tr>
<tr>
<td>2009</td>
<td>Contactless smart card operator case</td>
</tr>
<tr>
<td>2010</td>
<td>Contactless smart card operator case</td>
</tr>
<tr>
<td>2011</td>
<td>Contactless smart card operator case</td>
</tr>
<tr>
<td>2012</td>
<td>Contactless smart card operator case</td>
</tr>
<tr>
<td>2013</td>
<td>Contactless smart card operator case</td>
</tr>
<tr>
<td>2014</td>
<td>Contactless smart card operator case</td>
</tr>
<tr>
<td>2015</td>
<td>Contactless smart card operator case</td>
</tr>
</tbody>
</table>
Agenda

1. Regulations and Requirements of Data Privacy
2. Information Security Measures
3. The Amendment Ordinance
4. The System and Practices in the University
1. Regulations and Requirements of Data Privacy

‘Personal data’ means any data -

- (a) relating directly or indirectly to a living individual;
  - Indirect relationship; Remoteness
  - Direct relationship; Triviality
- (b) from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and
  - Practicable = reasonably practicable
  - Take into account all relevant data controlled by the party in question
    - Totality of such data
- (c) in a form in which access to or processing of the data is practicable.
  - Form refers to the physical shape, structure, type, etc. of the data in question
1. Regulations and Requirements of Data Privacy (cont’d)

**DPP1: Collection**
This provides for the lawful and fair collection of personal data and sets out the information a data user must give to a data subject when collecting personal data from the subject.

**DPP3: Use**
Unless the data subject gives consent, his/her personal data should only be used for the purposes for which they were collected or a directly related purpose.

**DPP2: Accuracy and Retention**
This provides that personal data should be accurate, up-to-date and kept no longer than necessary.

**DPP4: Security Safeguards**
This requires appropriate security measures to be applied to personal data (including data in a form in which access to or processing of the data is not practicable).

**DPP5: Transparency of Policies and Practices**
This provides for openness by data users about the kinds of personal data they hold and the main purposes for which personal data are used.

**DPP6: Access and Correction**
This provides data subjects with the rights of access to and correction of their personal data.
1. Regulations and Requirements of Data Privacy (cont’d)

► Practical Tips
► Remember to put PICS before the collection of personal data
► PICS should not be too vague or wide in scope
► Collect as little personal data as possible
► Allow certain personal data to be voluntarily collected
► HKID is considered to be sensitive personal data
1. Regulations and Requirements of Data Privacy (cont’d)

- Practical Tips
  - Get consent from data subjects if additional purposes
  - Privacy clauses with data processors
  - Direct Marketing
1. Regulations and Requirements of Data Privacy (cont’d)

► Practical Tips

► Data retention policy
► House keeping of personal data
► Ensure that personal data are accurate, i.e. Data validation in systems
1. Regulations and Requirements of Data Privacy (cont’d)

► Practical Tips

► Ensure that personal data are secure and protected against unauthorized or accidental access, processing, erasure or other use

► Examples of protection of personal data:
  ► Physical security
  ► Access control
  ► Secure storage and transmission
1. Regulations and Requirements of Data Privacy (cont’d)

- **Practical Tips**
  - A PPS should be made available to anyone, in an easily accessible manner, no matter whether personal data is collected by the data user in the physical world or in the online world.
  - If a data user operates a website, it is recommended that a web version of the PPS be made available by means of a prominent link at the top or at the bottom of the home page and every page of the website.
  - PPS should be linked directly.
1. Regulations and Requirements of Data Privacy (cont’d)

- Ensure that Data Access Request is performed according to procedure
  - Create a Data Access Request Form
  - Check the identity of the requestor
  - Response to a DAR within 40 days
  - Log book
  - Reasonable Fee

- Give the requestor a written notification with reasons if cannot comply with a DAR within 40 days
  - Exceptions to DAR
    - If the data user does not hold the requested data
    - If the requested data are “all personal data”
    - If the requested data comprise personal data of another individual
    - If the data user is unable to comply with a DAR within 40 days
2. Information Security Measures

- Data Classification - Identify / Manage / Protect Data

- Three Levels of Classification
  - Public
    - Open to Public
    - No Restriction on Access
  - Sensitive
    - Official Use Only
    - Protection due to proprietary, ethical or privacy considerations
  - Restricted
    - Protected by regulations, policies or contractual agreements
    - Unauthorized access may cause financial or reputational loss to HKU
2. Information Security Measures (Cont’d)

<table>
<thead>
<tr>
<th>Security Control</th>
<th>Public Level</th>
<th>Sensitive Level</th>
<th>Restricted Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Control</td>
<td>No restriction</td>
<td>AAA (Authentication, authorization, accounting)</td>
<td>AAA, Confidentiality agreement</td>
</tr>
<tr>
<td>Copying/Printing</td>
<td>No restriction</td>
<td>Limited</td>
<td>Limited with label “Confidential”</td>
</tr>
<tr>
<td>Network Security</td>
<td>No protection</td>
<td>Firewall, IPS, Allow remote Access</td>
<td>Firewall, IPS, No remote Access</td>
</tr>
<tr>
<td>System Security</td>
<td>Best practices</td>
<td>Hardening</td>
<td>Hardening with specific security</td>
</tr>
<tr>
<td>Physical Security</td>
<td>Locked</td>
<td>Locked, CCTV</td>
<td>Data Centre</td>
</tr>
<tr>
<td>Data Storage</td>
<td>Monthly Backup</td>
<td>Daily Backup</td>
<td>Encryption Data loss prevention Daily Backup</td>
</tr>
<tr>
<td>Auditing</td>
<td>No Logging</td>
<td>Logins</td>
<td>Logins, access and changes</td>
</tr>
</tbody>
</table>
2. Information Security Measures (Cont’d)

► Practical Tips
  ► Work Station
    ► Complex Password
    ► Enable login password and screen saver password
    ► Logout
    ► Avoid using public computer to access confidential files
    ► Physical Security
  ► Storage
    ► Encryption
    ► Backup
  ► Removable Storage
    ► Encryption
    ► Erase data after use
    ► Store sensitive data only when it is absolutely necessary
2. Information Security Measures (Cont’d)

► Practical Tips
  ► Cloud Storage
    ► Privacy and confidentiality
    ► Data Retention
    ► Exposure of data
    ► Data Encryption
  ► Social Network
    ► Privacy and Security Settings
    ► Manage your friends
  ► Mobile Security
    ► Enable Screen Lock
    ► Encrypt data
    ► Install mobile security apps
3. The Amendment Ordinance

► The Personal Data (Privacy) (Amendment) Ordinance 2012 (“Amendment Ordinance”) has come into effect on 1 October 2012.
► The Amendment Ordinance regulates all sale of personal data, use and transfer for the use of personal data in direct marketing and creates a new offence against the disclosure of personal data obtained without consent.
► The Amendment Ordinance places requirements to control over the use of data processors.
► The Amendment Ordinance empowers the Privacy Commissioner to assist data subjects in bringing proceedings to seek compensation from data users.
► The Amendment Ordinance imposes a heavier penalty (fine of up to HK$1,000,000 and imprisonment for up to 5 years) and creates a new offence against repeated contravention of enforcement.
3. The Amendment Ordinance (Cont’d)

- Making purchase and joining membership
- Offering of products and services, solicitation of donation to charity
- Provision of customer contact details to business partners
- Advertising of investment / insurance products
- Provision of customer contact details to agency for carrying out customer satisfaction survey
- Conduct of surveys for ABC Company

Use of personal data for direct marketing

Transfer of personal data to data processor

Provision of personal data for use in direct marketing
3. The Amendment Ordinance (Cont’d)

Use of personal data in direct marketing

**Provide Information to data subjects:**
► We intend to use your personal data for direct marketing
► We will use your name and phone number
► We may not use your personal data without your consent
► We may provide you with information relating to financial products and services

**Obtain oral consent from data subjects**
Within 14 days

**Obtain written consent from data subjects**

**Provide written confirmation to data subjects:**
► We have received your consent on 4 Mar 2014
► We will use your name and phone number for direct marketing
► We may provide you with information relating to financial products and services

**Use the personal data according to the confirmation**

**Do NOT use or provide personal data for direct marketing**

No consent can be obtained

**When receiving request from data subjects at any time to cease use**
3. The Amendment Ordinance (Cont’d)

Provision of personal data for use in direct marketing

Provide Information to data subjects:
► We intend to provide your personal data to our business partner within the insurance industry for use in direct marketing
► The provision will not be for monetary gain
► We will provide your name and address only
► We may not provide your personal data without your consent
► We may provide you with information relating to insurance products

Obtain written consent from data subjects

Provide personal data according to the consent

No consent can be obtained

Do NOT provide personal data for use in direct marketing

Notify data transferee in writing to cease the use of the personal data transferred for the purpose of direct marketing

When receiving request from data subjects at any time to cease providing the personal data
3. The Amendment Ordinance (Cont’d)

**Disclosure of personal data obtained without consent**

► Data user **must not disclose any personal data without the data subject’s consent** for monetary gains, or with an intent to cause loss in money/other property or psychological harm to the data subject.

► Consequence of non-compliance: criminal offence - fine of up to HK$1,000,000 and imprisonment for up to 5 years.
The System and Practices in the University


The System and Practices in the University

- Data Collection Statement
- Statutory Data Access / Correction Request Process
- University Data Protection Officer and Personal Data Protection Coordinators
- Information Technology Services (advice / security measures / guidelines / training information): http://www.its.hku.hk/services/training/infosec/personal-data-protection
- Central Compliance Team (compliance/monitoring)
The System and Practices in the University

The Public Expectation

Awareness and Education

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

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

© 2017 Ernst & Young, China
All Rights Reserved.

APAC no.
ED MMYY

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, or other professional advice. Please refer to your advisors for specific advice.

ey.com/china