Enforcing Data Protection
Receipt of Written Complaints

Complaint Screening

Screening Out

Complaint Handling

Conciliation Cases of Serious Nature

Conciliation successful

Conciliation unsuccessful

Non-compliance with enforcement notice

Civil Remedies

Apart from criminal sanction that may be imposed on a data user who has contravened a requirement under the Ordinance, an individual who suffers damage, including injury to feelings, by reason of such contravention, may seek compensation from the data user through civil proceedings.

Formal Investigation

Advisory Notice/Warning

No Contravention of the Ordinance

終結 Disposition

Refer cases to Police

Contravention of Provision of the Ordinance

Contravention of Data Protection Principles

Contravention of the Ordinance

Conciliation

End
The Operations Division receives and takes action on complaints lodged with the PCPD. We conduct investigations of suspected breaches of the Ordinance and take appropriate action to ensure compliance.

Impartial Investigation

The Operations Division receives and takes action on complaints lodged with the PCPD. We conduct investigations of suspected breaches of the Ordinance and take appropriate action to ensure compliance.
COMPLAINT INVESTIGATION

Data privacy complaints received

A total of 1,233 complaint cases were received in 2012-13, an 18% drop compared with that of the previous year. This can be explained by the exceptional increase in complaint cases in the previous year after the Octopus incident. (Figure 3.1)

Figure 3.1 - Number of Complaint Cases Received

<table>
<thead>
<tr>
<th>Year</th>
<th>Number of Complaint Cases</th>
</tr>
</thead>
<tbody>
<tr>
<td>2012-13</td>
<td>1233</td>
</tr>
<tr>
<td>2011-12</td>
<td>1507</td>
</tr>
<tr>
<td>2010-11</td>
<td>1225</td>
</tr>
<tr>
<td>2009-10</td>
<td>1022</td>
</tr>
<tr>
<td>2008-09</td>
<td>824</td>
</tr>
<tr>
<td>2007-08</td>
<td>834</td>
</tr>
</tbody>
</table>

The majority (73%) of the complaint cases (896) were made against private-sector organisations; 174 (14%) were against individuals; and 163 (13%) were against public-sector organisations, including government departments and public bodies. (Figure 3.2)

Figure 3.2 - Types of Parties Complained Against

<table>
<thead>
<tr>
<th>Type</th>
<th>Number of Complaint Cases</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private Sector</td>
<td>896</td>
</tr>
<tr>
<td>Individuals</td>
<td>174 (261)</td>
</tr>
<tr>
<td>Government Departments</td>
<td>123 (125)</td>
</tr>
<tr>
<td>Public Bodies</td>
<td>40 (27)</td>
</tr>
</tbody>
</table>

The drop in complaints in 2012-13 compared with the previous year can be explained by the exceptional increase in complaint cases in the previous year after the Octopus incident.
The private-sector organisations generating the most complaints were the banking and finance industry, followed by telecommunications and property management. The majority of the complaints made against companies in the telecommunications and financial sectors were about the alleged unlawful use or disclosure of their customers' personal data. (Figure 3.3)

**Figure 3.3 - Complaints Against Private-Sector Organisations**

<table>
<thead>
<tr>
<th>Sector</th>
<th>2012-13</th>
<th>2011-12</th>
</tr>
</thead>
<tbody>
<tr>
<td>Banking &amp; Finance</td>
<td>198</td>
<td>212</td>
</tr>
<tr>
<td>Telecommunications</td>
<td>123</td>
<td>112</td>
</tr>
<tr>
<td>Property Management</td>
<td>90</td>
<td>133</td>
</tr>
</tbody>
</table>

投訴個案數目 Number of Complaint Cases

The majority of complaints against public-sector organisations involved allegations of:

- use or disclosure of personal data beyond the scope of the collection purpose and without the consent of the individual (40%);
- excessive or unfair collection of personal data (25%);
- non-compliance with data access or correction requests (19%); or
- lack of security measures to protect personal data (11%).

Hospital / health service organisations, housing authorities and the police force generated the most complaints. (Figure 3.4)

**Figure 3.4 - Complaints Against Public-Sector Organisations**

<table>
<thead>
<tr>
<th>Sector</th>
<th>2012-13</th>
<th>2011-12</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hospital / Health Services</td>
<td>18</td>
<td>9</td>
</tr>
<tr>
<td>Housing</td>
<td>15</td>
<td>12</td>
</tr>
<tr>
<td>Police</td>
<td>14</td>
<td>25</td>
</tr>
<tr>
<td>Social Welfare / Social Work</td>
<td>8</td>
<td>9</td>
</tr>
<tr>
<td>Food and Environmental Hygiene</td>
<td>7</td>
<td>8</td>
</tr>
<tr>
<td>Leisure &amp; Cultural Services</td>
<td>6</td>
<td>10</td>
</tr>
</tbody>
</table>
Nature of Complaints

The 1,233 complaint cases received in 2012-13 involved a total of 1,622 alleged breaches of the requirements under the Ordinance. Of these, 1,305 (80%) were alleged breaches of the data protection principles (not a criminal offence) and 317 (20%) were alleged contraventions of the provisions of the Ordinance.

With regard to the nature of the complaints, the cases involved mostly the use of personal data without consent (567 alleged breaches), followed by complaints about the purpose and manner of data collection (510 alleged breaches), direct marketing (170 alleged breaches), compliance with data access or correction requests (146 alleged breaches), data security (133 alleged breaches), and accuracy and duration of retention (93 alleged breaches). Notwithstanding the overall downward trend, there were more complaints against the misuse of personal data for direct marketing purposes and complaints relating to data access or correction requests compared with the previous year. (Figure 3.5)

The number of allegations of data security and inaccuracy of personal data decreased by 38% and 24% respectively, compared with that of the previous year. There was a surge (45%) in the number of allegations of misuse of personal data in direct marketing activities. (Figure 3.5)
The upsurge of complaints relating to direct marketing is partly attributable to the commencement of the new direct marketing provisions of the Ordinance, which was implemented on 1 April 2013. It was observed that many organisations, for various reasons, sent notifications to their customers on use of personal data in direct marketing in late March 2013, and in many cases, the recipients mistook that sending the direct marketing notifications was contrary to the requirements under the Ordinance, and hence, lodged complaints with the PCPD.

Further, following the increasing popularity of smartphones to access the Internet, there was an upward trend in 2012-13 in the number of Internet-related complaints. Of the 64 Internet-related complaints, 19 concerned smartphone applications, 17 were about cyber bullying, and 16 related to social networks, such as the posting of personal data in discussion forums without the data subjects’ consent. (Figure 3.6)
In addition to the new complaints received, the PCPD handled 381 complaints carried forward from the previous year, bringing the total number of complaints handled during the year to 1,614. Of these, 1,221 (76%) cases were completed during the reporting year, and 393 (24%) cases were in progress on 31 March 2013.

### Summary of Complaints Handled in the year

<table>
<thead>
<tr>
<th></th>
<th>2012-13</th>
<th>2011-12</th>
<th>2010-11</th>
<th>2009-10</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Complaints Received</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>上年轉來的投訴</td>
<td>381</td>
<td>376</td>
<td>240</td>
<td>173</td>
</tr>
<tr>
<td>接獲的投訴</td>
<td>1233</td>
<td>1507</td>
<td>1225</td>
<td>1022</td>
</tr>
<tr>
<td>已完結的投訴</td>
<td>1221</td>
<td>1502</td>
<td>1089</td>
<td>955</td>
</tr>
<tr>
<td><strong>Complaints Outstanding</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>未完結的投訴</td>
<td>393</td>
<td>381</td>
<td>376</td>
<td>240</td>
</tr>
</tbody>
</table>

**Outcome of complaint handling**

Of the 1,221 cases completed during the reporting period, 179 (15%) were resolved through conciliation during the preliminary enquiry with the problems raised by the complainant remedied by the party being complained against; 80 (7%) were resolved after formal investigation; and 16 (1%) were transferred or reported to the Hong Kong Police Force (Figure 3.7).
Among the other cases which were not investigated:

- 399 (33%) cases involved mostly complaints where the matter had been dealt with by simply relaying the complainant’s concern to the party being complained against, or the complainant did not respond to the Commissioner’s inquiries after being invited to provide evidence to support the allegations;
- 189 (15%) were found to have no prima facie case;
- 120 (10%) were outside the jurisdiction of the Ordinance or were made anonymously;
- 128 (10%) were found to be unsubstantiated after enquiries with the party being complained against;
- 110 (9%) cases were withdrawn by the complainant during the preliminary enquiry.

We entered a new phase during the year with the Amendment Ordinance coming into force. The legislative process, from consultation to drafting and deliberation took as long as five years. It’s rewarding to see the outcome of all the effort my colleagues at the PCPD put into this. We produced leaflets and guidelines on the enhanced regulations on the use of personal data in direct marketing and on the legal assistance scheme. We anticipate privacy complaints to increase and more challenges ahead.
CASE STUDY: GUIDING DATA USERS TO IMPROVE

The Commissioner may decline to investigate a complaint under section 39 of the Ordinance. In such cases, the Commissioner’s decision and recommendation can still have a positive impact on data protection.

The following cases in the reporting year illustrate how the data user being complained against improved its data protection practices by taking measures under the Commissioner’s guidance.

投訴內容

The Complainant was a policyholder of an insurance company (“the Company”) and had instructed the Company to discharge Agent A as her insurance agent. However, the Complainant continued to receive promotional materials from Agent A under the Company’s name. The Complainant therefore complained against the Company for allowing Agent A, who was no longer her insurance agent, to continue to access and use her policy-related personal data.

In response to the PCPD’s enquiry, the Company explained that it was its practice to allow former insurance agents (who had first signed the customer up with the Company) and their supervisors to access customers’ policy-related personal data from the Company’s database in order to follow-up with policy-related matters.

Outcome

The Commissioner held that it was reasonably practicable for the Company to arrange disclosure of relevant policy-related data only when such needs arise, and that the Company’s granting of indiscriminative access rights to policy related data to insurance agents and their supervisors of former customers under the circumstances of the case had violated DPP3.

The Company accepted the Commissioner’s recommendations and undertook to review its access-rights mechanism, remove the access right of former insurance agents and their supervisors, and allow only current insurance agents and their supervisors to access and use the personal data of their policyholder customers. The Company also issued notices to all of its insurance agents to put into effect this instruction.
A Bank should ensure the consumer credit data it provided to credit reference agency was accurate - DPP2(1)

The Complaint

The Complainant entered into a debt restructuring agreement (“the 2003 Agreement”) with the Bank with respect to two bank accounts he had opened at the bank in 2003. The Complainant could not repay the monthly amount as required, and the debt restructuring agreement failed. In 2006, the Complainant made a monthly repayment agreement (the “2006 Agreement”) with the Bank over the phone, and thereafter made repayment accordingly.

A few years later, the Complainant obtained his personal credit report from TransUnion Limited (“TransUnion”), and he found that the Bank (i) had not provided to TransUnion the information about the 2003 Agreement and the 2006 Agreement; and (ii) had reported inconsistent information about the number of days past due (including 30 days and 1 day) to TransUnion regarding one of the bank accounts.

The Bank explained that after it made the 2003 Agreement with the Complainant, it had regularly reported the repayment records of the Complainant to TransUnion. However at that time the Bank’s system did not support the reporting of debt repayment arrangement (including Individual Voluntary Arrangement) between the Bank and its clients, and therefore it did not notify TransUnion of the information about the 2003 Agreement. Furthermore, the Bank considered that the 2006 Agreement was a verbal agreement made over the phone, other than a formal debt arrangement so that it did not notify TransUnion of the related information.

Moreover, the Bank claimed that after it made an Individual Voluntary Arrangement with a client, it would write off the payment in default in his account. Since TransUnion set the number of days past due for a write-off account should not equal to “0”, the Bank reported the minimum number of days past due to be “1 day” until the client settled all the amounts in default. The Bank explained that as it received repayment from the Complainant in relation to the accounts, it reported to TransUnion that the number of days past due was changed from “30 days” to “1 day” for the account, and throughout the repayment period continued to notify TransUnion that the account had “1 day” past due until the Complainant settled all the payments in default.
Outcome

The Commissioner held that even though the 2006 Agreement was not made in accordance with the formal procedure for repayment agreement that the Bank referred to, considering that the Bank subsequently accepted the mode of repayment under the agreement and continued to manage the relevant accounts (including the due date and instalment), and that the Bank also recorded the 2006 Agreement, the nature of the repayment agreement was by no means different from a debt restructuring or a re-arrangement. Hence in this case the Bank’s failure to notify TransUnion of the 2003 Agreement and the 2006 Agreement was a contravention of the requirements of the Code of Practice on Consumer Credit Data.

As regards the fact that the Bank had set “1 day” as the minimum day of past due of a write-off account, TransUnion, following the PCPD’s compliance check, had notified its members (including the Bank) in 2008 that they should terminate the write-off account after the account was entered into a debt restructuring arrangement, and should open an evolving credit account so as to report to TransUnion whether overdue repayment still existed in the account concerned after entering into the debt restructuring arrangement. In this regard, the Commissioner considered that the Bank’s notification to TransUnion of the Complainant having a record of “1 day” past due while the Complainant made repayment on time did not accurately reflect the repayment status of the Complainant.

Accordingly, the Bank had asked TransUnion to delete the account information that involved inaccurate reporting, and undertook to the Commissioner that it would notify TransUnion of any debt arrangement including verbal repayment agreement it made with its clients.
RESULTS OF INVESTIGATIONS OF COMPLAINT CASES

Results of Formal Investigations

The PCPD completed 80 formal investigations during the reporting period. In 11 cases (14%), it found a contravention of the requirements under the Ordinance; in 12 cases (15%), either no contravention was found or no contravention was established due to insufficient evidence. The remaining 57 cases (71%) were discontinued for various reasons, such as the dispute between the parties having been resolved through conciliation or the complainant having decided not to pursue the matter further during the investigation (Figure 3.8).

Figure 3.8 - Results of Formal Investigations

![Figure 3.8 - Results of Formal Investigations](image-url)
Of the 11 cases where the requirements under the Ordinance were found to have been contravened, nine involved a contravention of one or more of the Data Protection Principles. The remaining two cases involved contravention of the requirements under the main body of the Ordinance relating to compliance with data access requests (Figure 3.9).

<table>
<thead>
<tr>
<th>Nature of Contravention</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collection &amp; Purposes</td>
</tr>
<tr>
<td>Use Without Consent</td>
</tr>
<tr>
<td>Access Request</td>
</tr>
<tr>
<td>Accuracy &amp; Retention</td>
</tr>
<tr>
<td>Inadequate Security</td>
</tr>
<tr>
<td>Direct Marketing</td>
</tr>
<tr>
<td>Openness of Data Policy</td>
</tr>
</tbody>
</table>

Enforcement action
The PCPD takes enforcement action in cases of contravention.

Of the 11 cases found to have contravened the requirements under the Ordinance, the Commissioner issued enforcement notices to the parties complained against in seven cases to stop or prevent the contraventions. In the remaining four cases, the Commissioner issued warning notices to the parties complained against after they had taken measures to remedy the contraventions.

Other action taken as a result of complaints
In the 179 cases resolved through conciliation during preliminary enquiries, the Commissioner provided advice and/or recommendations to 160 organisations on their practices and procedures to assist them in complying with the Data Protection Principles and other requirements of the Ordinance.

Of the 57 formal investigations discontinued during the reporting period, the Commissioner saw fit to issue warning notices to the parties complained against in 22 cases.
PROSECUTION AND CONVICTION CASES

During the year, there was no complaint case which involved contravention of the provisions in the main body of the Ordinance, leading to conviction. However, one person was charged under section 50B(1)(a) [formerly section 64(9)] with the offence of obstructing a PCPD officer whilst serving summonses to two staff members of an organisation under section 44(1) of the Ordinance in the course of investigating complaints. The defendant was an on-duty office assistant of the organisation.

At the hearing in June 2012 at the Kwun Tong Magistrates’ Courts, the Prosecution and the Defence agreed to an O.N.E. (Offer No Evidence) Bind Over on the basis that the defendant had pleaded not guilty while agreeing with the facts of the case, and the Magistrate ordered the defendant to pay a surety of HK$2,000 and to be bound over for 12 months.

PUBLICATION OF INVESTIGATION REPORT UNDER SECTION 48(2)

Investigation Report: A Medical Check-up Service Company and an Insurance Broker Collected Personal Data for Use in Direct Marketing by Arguably Deceitful Means

The Commissioner initiated a formal investigation against Hong Kong Preventive Association Limited (“HKPA”) and Aegon Direct Marketing Services Insurance Broker (HK) Limited (“Aegon Direct”) in respect of three complaints.

Over the previous two years, HKPA had obtained personal data from about 360,000 people and sold the data to Aegon Direct for use in the direct marketing of insurance products. The PCPD received 11 enquiries and five complaints in this regard.

Release of the investigation report at a media conference.
The PCPD’s investigation found that both companies, as data users, had contravened the Data Protection Principles (“DPPs”) set out in the Ordinance:

**HKPA**
- HKPA’s telemarketers offered a free medical check-up in support of a “universal medical check-up scheme” which did not exist and misled the complainants into believing that the scheme had the blessing of the Government. It failed to explain clearly that the data would be transferred to Aegon Direct for use in direct marketing activities. Such unfair means of collection constitutes a contravention of DPP1 (2) [on Data Collection];
- HKPA failed to take all practicable steps to explicitly inform the complainants of its intention to transfer their personal data to a third party, and when mentioning Aegon Direct as the transferee, it did not say what kind of business Aegon Direct was engaged in. It thus contravened DPP1 (3) [on Data Collection]; and
- Such transfer of the complainants’ personal data was neither consistent with, nor directly related to, the original purpose of the data collection (namely, registration for a free medical check-up). As this was done without the explicit and voluntary consent of the complainants, it constituted a contravention of DPP3 [on Data Use].

**Prevention Association**
- Prevention Association’s telemarketers had offered a free medical check-up in support of a “universal medical check-up scheme” which did not exist and misled the complainants into believing that the scheme had the blessing of the Government. It failed to explain clearly that the data would be transferred to Aegon Direct for use in direct marketing activities. Such unfair means of collection constitutes a contravention of DPP1 (2) [on Data Collection];
- Prevention Association failed to take all practicable steps to explicitly inform the complainants of its intention to transfer their personal data to a third party, and when mentioning Aegon Direct as the transferee, it did not say what kind of business Aegon Direct was engaged in. It thus contravened DPP1 (3) [on Data Collection]; and
- Such transfer of the complainants’ personal data was neither consistent with, nor directly related to, the original purpose of the data collection (namely, registration for a free medical check-up). As this was done without the explicit and voluntary consent of the complainants, it constituted a contravention of DPP3 [on Data Use].

---

**Assessing the PCPD’s Current Practices…** Within these constraints (the Commissioner) seems to be making vigorous use of his powers, as indicated by the increasing use of all of the enforcement mechanisms of the Ordinance over the past 18 months. He has also been looking for more effective ways to use additional powers, of which the making of detailed s48(2) “name and shame” reports is a high value example…The PCPD’s reporting practices are at least as informative as other Asian jurisdictions, and are comparable with the best practices of DPAs globally.

---

**Professor Graham Greenleaf**

Austere Institute of Technology & Information Systems, University of New South Wales

(cited from Professor Greenleaf’s article “Hong Kong’s data protection enforcement: More bark and bite” published in Privacy Laws and Business International Report, August 2013)
**Aegon Direct**

- The collection of partial identity card numbers from the complainants was held to be excessive, as the other contact data supplied already sufficed for the purpose of authenticating the claimants for the free medical check-up and preventing multiple claims. This constituted a contravention of DPP1(1) [on Data Collection]; and

- Without the complainants’ voluntary and explicit consent, it used their personal data for direct marketing: a purpose which was different from, and not directly related to, the original purpose of the data collection (namely, registration for a medical check-up), thus contravening DPP3 [on Data Use].

- After the PCPD’s intervention, Aegon Direct ceased using the complainants’ personal data for direct marketing, and destroyed their personal data records, as well as the records of partial identity card numbers, of persons who had not purchased any insurance products through Aegon Direct.

However, in order to remedy the contraventions and prevent any recurrence, the Commissioner served on HKPA and Aegon Direct an enforcement notice directing both companies to formulate relevant policies, guidelines and/or procedures to prevent any contraventions of the requirements under Part VIA of the Ordinance when they collect and use personal data for direct marketing purposes in future.

The Commissioner also directed Aegon Direct to destroy the personal data provided by HKPA in six months’ time, (a) except the personal data of the data subjects who, as a result of HKPA’s referral, had purchased insurance products through Aegon Direct, and (b) unless such data would be used for direct marketing before expiry of these six months, in which case the provisions in Part VIA of the Ordinance must be complied with. Aegon subsequently complied with the enforcement notice by destroyed the data concerned.
Every investigation involves the painstaking process of evidence gathering and thoughtful analysis. In one investigation I took part in recently, I was required to listen to voice recordings of conversations between the complainants and telemarketers of the company complained against. When the telemarketers in question explained what the complainants’ personal data was being collected for, they spoke so fast that it was very difficult to follow. Even though I paid very close attention to the recordings, it was very hard to grasp the message. The investigation ended up determining that the collection of personal information in such a way was a contravention, and I was assigned to deliver the Enforcement Notice to the company.

"每項調查結果背後都需要調查人員抽絲剝繭，慎思明辨。早前我參與一宗案件的調查工作，我需要聽取多段投訴人與電話推廣員的電話錄音，推廣員草草交代收集個人資料的用途，或加快語速，甚至含糊其辭，即使我已全神貫注聆聽，也難以掌握他們欲表達的訊息。公署裁定這種收集個人資料的手法違反條例的規定，並由我親手向違規機構送遞執行通知。"
Excessive collection of customers’ Hong Kong Identity Card numbers for authentication purposes by a beauty centre - DPP1(1)

The Complaint
The Complainant, a customer of a beauty centre (the “Beauty Centre”), was required to provide her Hong Kong Identity Card number (“ID card number”) for online appointment bookings at the Beauty Centre. The Complainant considered the collection of her ID card number to be excessive, so she lodged a complaint with the PCPD.

Outcome
The Commissioner’s investigation revealed that the Beauty Centre had issued a membership card to individual customers bearing the customer’s photo and a unique membership number. The Commissioner was of the view that the collection of customers’ ID card numbers for authentication purposes was unnecessary and excessive, as the membership card number sufficed for the same purpose. Even if the Complainant could not produce her membership card on the spot, the Beauty Centre could ask for her name, telephone number and address to verify her identity. Therefore, the Beauty Centre had contravened DPP1(1).

In the course of the investigation, the Beauty Centre ceased the practice of collecting ID card numbers from customers and destroyed the records of ID card numbers previously collected to remedy the contravention. In the circumstances, the Commissioner decided to put the Beauty Centre on warning instead of serving an enforcement notice on it.
Excessive collection of locker users' Hong Kong Identity Card numbers for security purposes by a public sports centre - DPP1(1)

The Complaint

In response to the Complainant’s request for use of a locker in a public sports centre, the serving staff asked for his Hong Kong Identity Card number ("ID card number"). The Complainant questioned the necessity of collecting his ID card number, as he had already provided his name and telephone number when registering for use of the locker.

The sports centre explained to the Commissioner that the collection of ID card numbers from locker users enhanced the management and security of the sport facility. However, the sports centre was unable to provide any information about suspected crimes committed by locker users.

Outcome

The Commissioner was of the view that the sports centre could not collect locker users’ ID card numbers solely because of potential risk of crime committed by them. If locker users reported the loss of their locker keys, the most effective way to identify the locker users was to ask them to give the names and telephone numbers they provided upon registration for verification. If the sports centre still doubted their identity, it could also ask them to produce an identification document bearing their photos for verification.

The Commissioner concluded that the sports centre’s collection of ID card numbers of locker users had contravened DPP1(1). An enforcement notice was served on the sports centre directing it to cease the practice and destroy all records of ID card numbers so collected. The sports centre complied with the enforcement notice.
An employer disclosed copies of the marriage certificate of a former employee to third parties – DPP3.

The Complaint

The Complainant was employed by a recruitment company (the “Company”) on an employment visa. Prior to her resignation, the Complainant applied for marriage leave and produced a copy of her marriage certificate (the “Certificate”) to the Company as proof of her marriage. Subsequently, the Company and the Complainant had a labour dispute.

During a hearing at the Labour Tribunal, the Complainant learned that the Company had disclosed the Certificate to the Immigration Department in connection with the cancellation of her employment visa and that the Company had disclosed the Certificate to the Labour Department to object to the grant of an employment agency license to a recruitment company run by the Complainant and her husband. Hence, the Complainant lodged a complaint with the PCPD against the Company for disclosing the Certificate to third parties without her prior consent.

Outcome

The Commissioner’s investigation revealed that for the purpose of withdrawing sponsorship for the working visa of an employee, a written notification by the employer to the Immigration Department would suffice. Therefore, it was unnecessary for the Company to furnish a copy of the Certificate to the Immigration Department for the purpose of withdrawing its sponsorship.

On the other hand, the Commissioner noted that in accordance with section 53(1) of the Employment Ordinance, the Labour Department may only refuse or revoke the employment agency license of the Complainant’s company if “within the preceding five years, (the Complainant) has been convicted of an offence against a child, young person or woman, or of an offence involving membership in a triad society, fraud, dishonesty or extortion”. The Commissioner held that the dispute between the Company and the Complainant concerned only the breach of employment contract terms, duty of confidentiality and restrictive covenants, which did not fall within any of the specified situations under section 53(1) of the Employment Ordinance.
Since the Certificate was collected by the Company in the course of and for the purpose of human resource management to assess the Complainant’s entitlement to marriage leave, the subsequent disclosure of the Certificate to the two government departments by the Company was inconsistent with or did not bear any direct relationship with the purpose for which the Certificate was first provided to the Company by the Complainant. The Commissioner therefore found the Company in contravention of DPP3 and issued an enforcement notice to the Company to remedy the breach.
A school refused data access requests made by two teachers without carefully considering whether the exemptions of sections 58(1)(d), (e) and (f) were applicable.

The Complaint

Two Complainants, who were teachers at the school concerned, made data access requests (the “DARs”) to the school for their personal data contained in documents in relation to disciplinary action carried out by the school against them. The DARs were refused by the school on the ground that the requested data was exempt from sections 58(1)(d), (e) and (f) of the Ordinance. The Complainants were dissatisfied with the school’s replies and lodged complaints with the PCPD against the school.

During the course of the investigation, the school submitted that provision of the concerned documents would reveal the identities of the students and teachers who had complained against the Complainants and that complying with the DARs would prejudice the purpose of rectifying the improper conduct and the monitoring of the behaviour of the Complainants. The school thus invoked section 58(1)(d) of the Ordinance to refuse to comply with the DARs. The school further submitted that the disclosure of the concerned documents to the Complainants would result in significant loss to the school within the terms of section 58(1)(e) of the Ordinance, that the morale of the teaching staff would be adversely affected, and that the school might be subject to litigation/legal action by the parties whose identities were thereby revealed. The school also relied on section 58(1)(f) of the Ordinance that the concerned documents were held to ascertain whether the misconduct of the Complainants was likely to have a significant adverse impact on the school in the exercise of its management functions.

Outcome

The Commissioner took the view that, in respect of the applicability of section 58(1)(d) of the Ordinance, the behaviour of the Complainants did not amount to “serious improper conduct”, as the disciplinary action taken against them was merely a warning.
Furthermore, the school only speculated about "significant financial loss". The Commissioner considered that the potential "loss" asserted was too remote and did not satisfy the requirement of section 58(1)(e) of the Ordinance. Likewise, as the school had failed to prove how the misconduct of two individual teaching staff would have a significant adverse impact on the school’s management functions, and the Commissioner dismissed the ground for exemption under section 58(1)(f) of the Ordinance. Hence, the Commissioner concluded that the school had failed to fulfil the statutory requirements of section 19(1) of the Ordinance.

An enforcement notice was served on the school directing it to comply with the DARs and devise guidelines for handling DARs for its staff to follow. The school agreed with the direction given by the Commissioner and complied with the enforcement notice accordingly.