PART V: DIRECTIONS TO SECURE COMPLIANCE

23. Power to issue directions to secure compliance

23.1 The Commission's power to issue directions to secure an organisation's compliance with the Data Protection Provisions is set out in section 29 of the PDPA. In particular:

23.1.1 Section 29(1) of the PDPA provides that the Commission may, if it is satisfied that an organisation is not complying with any of the Data Protection Provisions, give the organisation such directions as the Commission thinks fit in the circumstances to ensure the organisation's compliance with that provision.

23.1.2 Section 29(2) of the PDPA further provides that the Commission may (without prejudice to section 29(1) of the PDPA) give an organisation that is not complying with any of the Data Protection Provisions any or all of the following directions:

(a) to stop collecting, using or disclosing personal data in contravention of the PDPA;

(b) to destroy personal data collected in contravention of the PDPA;

(c) to comply with any direction of the Commission under section 28(2) of the PDPA; or

(d) to pay a financial penalty of such amount not exceeding $1 million as the Commission thinks fit.

23.2 In general, the directions that the Commission may give under section 29 of the PDPA are likely to fall within the following types:

23.2.1 directions to remedy the organisation's contravention, that is, by requiring the organisation to take corrective action, for example, by requiring the infringing organisation to cease its use of personal data collected in contravention of the PDPA;

23.2.2 directions to prevent or reduce the possibility of harm (or further harm) to individuals who are (or may be) affected by the organisation's contravention;

23.2.3 directions to rectify an organisation's processes, for example, by requiring the infringing organisation to take certain measures so that it will be brought into compliance with the Data Protection Provisions; and

23.2.4 directions to impose a financial penalty.

23.3 In the event an organisation does not comply with a direction under section 29 of the PDPA, the Commission is empowered under section 30 of the PDPA to enforce the direction by registering it in the District Court. Please refer to section 27 of these Guidelines for more information on the enforcement of the Commission's directions.

24. Directions to pay financial penalties

24.1 In considering whether to direct an organisation to pay a financial penalty, the Commission will take into account certain factors, such as the seriousness and impact of the organisation's breach and the immediacy and effectiveness of corrective actions that the organisation took to address the breach. The Commission may also consider if the organisation had acted deliberately, wilfully or if the organisation had known or ought to have known of the risk of a serious contravention and failed to take reasonable steps to prevent it.

24.2 The Commission will determine each case on its own merits and circumstances. However, the Commission will also adopt an objective approach to assessing the seriousness of a breach of the Data Protection Provisions, by considering how a reasonable organisation should behave in a particular situation.

25. How financial penalties are determined

25.1 In this section, the Commission sets out a non-exhaustive list of some aggravating and mitigating factors that the Commission may consider when it calculates a financial penalty.

Aggravating factors

25.2 Some of the factors that the Commission may consider to be aggravating factors include, but are not limited to:

25.2.1 the organisation failed to actively take reasonable steps to resolve the matter with the individual in an effective and prompt manner;

25.2.2 intentional, repeated and/or ongoing breaches of the Data Protection Provisions by an organisation. This would include situations where the organisation knew, or ought reasonably to have known, of the risk of a breach, or breach of the Data Protection Provisions but continued with its operations without taking measures to minimise the risk or remedy the breach;

25.2.3 obstructing the Commission during the course of investigations (such as making efforts to withhold or conceal information requested by the Commission);

25.2.4 failing to comply with a previous warning or direction from the Commission; and

25.2.5 the organisation is in the business of handling large volume of sensitive personal data, the disclosure of which may cause exceptional damage, injury or hardship to a person (such as medical or financial data), but failed to put in place adequate safeguards proportional to the harm that might be caused by disclosure of that personal data.

Mitigating factors

25.3 Some of the factors that the Commission may consider to be mitigating factors include, but are not limited to:

25.3.1 the organisation has actively and promptly resolved the matter with the individual;

25.3.2 the organisation has taken reasonable steps to prevent or reduce the harm of a breach (such as putting in place strong passwords to prevent unauthorised access);

25.3.3 the organisation has engaged the individual in a meaningful manner and has voluntarily offered a remedy to the individual, and that individual has accepted the remedy;

25.3.4 the organisation took immediate steps to notify affected individuals of the breach and reduce the damage caused by a breach (such as informing individuals of steps they can take to mitigate risk); and

25.3.5 the organisation voluntarily notified the Commission of the personal data breach as soon as it learned of the breach, and co-operated with the Commission in its investigations.