Code of Practice
on Protection of Customer Information for
Fixed and Mobile Service Operators

Introduction

In the course of their business and provision of services, fixed[1] and mobile[2] service operators collect a large volume of customer personal data. Some of these data, including ***a customer's telephone number***, ***residential address*** and ***details of call history***, may be sensitive in certain circumstances and of value if used for illicit purposes. A service operator should therefore ensure that data relating to customers are properly protected from misuse otherwise the reputation of the company will be tarnished by dishonesty and corruption.

Objective

2. This voluntary Code of Practice, which sets out some good practices for preventing unauthorized disclosure of customer information by staff, serves as a general guidance for fixed and mobile service operators to set their standards and measures in respect of protection of customer information. The good practices suggested are not exhaustive. Fixed and mobile service operators may adopt other standards and measures which can provide reasonably sufficient protection to customer information. In addition, fixed and mobile service operators are reminded to observe the requirements of the legal provisions relating to privacy of personal data and prevention of bribery.

---

[1] For the purpose of this Code of Practice, fixed service operator means the holder of a Fixed Carrier Licence or a Fixed Telecommunications Network Services Licence granted by the Telecommunications Authority under the Telecommunications Ordinance (Cap. 106) for the provision of local fixed telecommunications network service.

[2] Mobile service operator means the holder of the following licences granted by the Telecommunications Authority under the Telecommunications Ordinance (Cap. 106):

(a) a Mobile Carrier Licence for the provision of public radiocommunications service using cellular technology in the 1.9GHz – 2.2GHz band;

(b) a Public Radiocommunications Services Licence for the provision of public radiocommunications service using cellular technology in the 800/900MHz, 1.7-1.9GHz band or public radio paging service; or

(c) a Public Non-Exclusive Telecommunications Services Licence for the provision of mobile virtual network service.

Legislation

Personal Data (Privacy) Ordinance

3. Section 4 of the Personal Data (Privacy) Ordinance (Cap. 486) requires that a data user shall not do an act, or engage in a practice, that contravenes a data protection principle listed in Schedule 1 of the Ordinance unless the act or practice, as the case may be, is required or permitted under the Ordinance. Principle 4, among the six Data Protection Principles, is of particular relevance to this Code of Practice and requires that:

> All practicable steps shall be taken to ensure that personal data (including data in a form in which access to or processing of the data is not practicable) held by a data user are protected against unauthorized or accidental access, processing, erasure or other use having particular regard to -
>
> (a) the kind of data and the harm that could result if any of those things should occur;
>
> (b) the physical location where the data are stored;
>
> (c) any security measures incorporated (whether by automated means or otherwise) into any equipment in which the data are stored;
>
> (d) any measures taken for ensuring the integrity, prudence and competence of persons having access to the data; and
>
> (e) any measures taken for ensuring the secure transmission of the data.

4. A breach of a data protection principle is not by itself an offence. However, the Privacy Commissioner for Personal Data may, in certain circumstances, require compliance with such a principle by means of an enforcement notice. A breach of such a notice is an offence. In addition, an individual that suffers damage, including injury to feelings, as a result of a breach of a requirement of a data protection principle in relation to data of which he or she is the subject, has a right to compensation. An employer may be liable for any act of an employee causing such damage.

Prevention of Bribery Ordinance

5. Section 9(1) of the Prevention of Bribery Ordinance (Cap. 201) states that any agent who, without lawful authority or reasonable excuse, solicits or accepts any advantages as an inducement to or reward for or otherwise on account of his

(a) doing or forbearing to do, or having done or forborne to do, any act in relation to his principal's affairs or business; or

(b) showing or forbearing to show, or having shown or forborne to show, favour or disfavour to any person in relation to his principal's affairs or business,

shall be guilty of an offence. Therefore, unauthorized disclosure of customer personal data by staff of fixed and mobile service operators in return for an advantage may breach the provisions of the Prevention of Bribery Ordinance.

Licence Condition

6. Telecommunications licences have a licence condition which provides that the licensee shall not disclose information of a customer except with the consent of the customer, which form of consent shall be approved by the Telecommunications Authority and that the licensee shall not use information provided by its customers or obtained in the course of provision of service to its customers for purposes other than those related to the provision of service by the licensees.

Good Practices

7. The following good practices provide general guidance to assist fixed and mobile service operators to prevent unauthorized disclosure of customer information by their staff. They could be classified into five major categories:

(a) Policy on Protection of Customer Personal Data;

(b) Technical Measures for Protection of Customer Personal Data;

(c) Location Security;

(d) Staff Security; and

(e) Transfer of Customer Personal Data

A. Policy on Protection of Customer Personal Data

Data Classification Policy

8. Service operators collect personal data (e.g. name, identity document number, residential address, etc.) from customers when the latter subscribe to services. Service operators also generate other personal data (e.g. service plan details, usage details, billing details, payment details, etc.) during the course of provision of services. Since personal data are of different degrees of sensitivity in different contexts, service operators should establish a data classification policy which suitably classifies the various kinds of personal data they hold, based on their degree of sensitivity and risk of exposure. The policy should also define security measures that should be put in place to safeguard each classification of personal data, be they in electronic form or in paper format. The objective of the policy is to prevent unauthorized disclosure of customer information by staff.

Ethics and Data Privacy Policy

9. A service operator should establish an ethics policy laying down the ethical standards of the company with particular regard to the protection of customer personal data. This could be in the form of a data privacy policy that explicitly states that both as a moral obligation and as a legal requirement under the Personal Data (Privacy) Ordinance, the company is committed to protecting customer personal data from unauthorized disclosure. A service operator should provide its employees, whether local or off-shore, with explicit guidelines on maintaining confidentiality of customer personal data. An employee should also be required to undertake, say by means of relevant provisions in the employment contract, to hold information to which he or she has access in the strictest confidence and not to use it for any purpose except as required in the proper discharge of his or her duties as an employee of the service operator. The policy should also address the importance of prevention of bribery.

10. The ethics policy should be promulgated to all staff and both newly recruited and serving staff should be regularly reminded to comply with the requirements. To ensure compliance, a service operator should give a clear warning of the disciplinary actions and criminal sanctions, as applicable, that will be taken against an employee who fails to comply with the requirements.

Access Control Policy

11. In daily business operations, different staff require different types of access (e.g. read only, read write) to different types of personal data. Providing an employee with access rights that exceed what he or she is required to enable him or her to carry out his or her daily business operations creates an unnecessary opportunity for abuse. Service operators should establish an access control policy setting out the levels of authority and the associated types of access rights for each category of personal data. In general, access to data should be given on the basis of a practical application of the "Need-to-know" principle. If computer applications are used to facilitate processing and retrieval of customer personal data, access to functions should be given on a "Need-to-do" principle. Owing to the wide use of personal computers, service operators should also consider controlling on-line printing and down loading of customer personal data to local personal computers or magnetic media, for these activities leave no trail for auditing the use of the data so printed or down loaded. There should be explicit limits on the duration of storage/file keeping of materials containing customer personal data, be they in electronic form or paper format.

B. Technical Measures for Protection of Customer Personal Data

Access Authorization System

12. A service operator should establish an access authorization system laying down the application procedures for access rights to customer personal data, be they in electronic or paper form, and with the appropriate levels of approving authority clearly defined. All applications must be properly approved before access rights are given. Measures ensuring the confidentiality of correspondence (e.g. use of sealed envelopes and requirements to acknowledge receipt), if applicable, should be in place. To promote compliance, details of the access authorization system should be well promulgated among all staff members.

Identification and Authentication

13. To ensure accountability, staff members having access to customer personal data should each be given a user account of their own. They should be required to identify themselves to the system as a valid user by using their unique user IDs and authenticate themselves with valid passwords before they can have further access to prescribed system functions. They should be regularly reminded not to disclose their

passwords to others and to log off the system immediately after use to avoid leaving their accounts open for others to use. A service operator should also reconcile valid user accounts on a regular basis to avoid abuse of obsolete user accounts as a result of staff turnover.

Password Management

14. To minimize disclosure of password, password management controls should be imposed, such as : not using dates and obvious words as passwords; setting a minimum length of passwords; periodic ageing of passwords; compulsory changing of passwords upon first log on and after every reset; inhibiting re-use of old passwords within a specific cycle; and deactivating a user account upon a specified number of invalid log on attempts.

Access to Customer Information

15. As a means to verify the legitimacy of a customer when asking for a service, it is common practice to require a customer to identify and authenticate himself or herself before a service is to be provided. For example: a paging services customer is usually required to quote his or her account number and password before he or she may check for messages deposited in his or her account; a mobile phone service customer is usually required to quote his or her telephone number and identity document number before he or she can change a service plan. To prevent front line customer services staff from retrieving customer personal data other than in response to a customer's request, a composite key should be used for retrieving customer personal data. For example, a good security feature for online access would be the use of multiple identification codes in which one of the codes is a unique PIN issued and known only to the customer for the purpose of accessing information relating to his or her account. Customer should be provided with facilities so as to change the PIN to a number of his or her own choice.

16. To enable tracking of activities performed by staff members during the course of access of customer information, a service operator should as far as it is practicable to do so consider maintaining audit trails of all activities performed by authorized users, including enquiry activities. Audit trails on unauthorized access attempts should also as far as it is practicable to do so be maintained. These records should be retained for a reasonable period of time to assist in future investigations and access control monitoring. In addition, they should be protected from any alterations and subject to supervisory checks.

17. A service provider is encouraged as far as it is practicable to do so to take an active approach to adopt the measures mentioned above in respect of access to customer information. The cumulative effects of the measures proposed in paragraphs 15 and 16 would depend on whether or not the operators are able to take all or some of the proposed measures. It is considered that if any of the above positive measures are not carried out, a reactive approach should at least be in place such that in case of fault discovery or complaints received against abuse of authorization to access customer information by staff a service provider can readily identify means to facilitate investigation and prevent further abuse.

Security of Connection

18. The staff of retail shops may require remote access to the service operator's computers. A service operator should check that requests for connection are from known and authorized locations. Where the information requires additional protection, a service operator should encrypt transmissions to make the data unintelligible in the event of interception.

Document Security

19. Completed service application forms, computer generated reports and other kinds of documents may contain customer personal data. A service operator should take all practicable steps to guard against unauthorized access to these documents. A service operator should take all reasonably practicable steps to ensure that such documents are disposed of in a secure manner without disclosing customer personal data. For example, a service operator should maintain a complete record on any physical transfer of documents containing customers' data that may occur upon the moving or closing of any shops, identifying in such record the relevant documents, the date of transfer and destination.

Copies of Identity Documents

20. A service operator may collect copies of identity cards, or other identity documents, from its customers as a result of subscription to the services. Unauthorized access to such documents creates an unnecessary opportunity for abuse. To prevent malpractice, copies of such documents should be collected on a necessary and justifiable basis, marked with the word "COPY" across the images of the identity documents, treated as confidential documents, stored in secure locations with restricted access, not

retained longer than necessary, and disposed of securely. Further guidance on the collection and use of copies of identity cards can be found in the Code of Practice on the Identity Card Number and other Personal Identifiers issued by the Office of the Privacy Commissioner for Personal Data.

C. Location Security

Computing Centres

21. Computing centres where computing facilities are located, offices where workstations are located and documents are kept, telephone exchanges and junction boxes where cables route through are areas where customer personal data can be obtained by means of theft, interception or phone bugging. Physical access to these locations must therefore be controlled and monitored and access should be restricted to authorized personnel only.

Peripheral Equipment

22. A service operator who allows service applications to be submitted by means of fax should use a dedicated fax machine and should not locate the equipment in open areas to which access is not restricted. A service operator should also pay attention to the positioning of workstations *or consider using screen saver* so that customer personal data will not be seen by unauthorized parties during data processing.

D. Staff Security

Security Training

23. The effectiveness of security measures relies on staff compliance. A service operator should implement a corporate training policy to provide adequate security education and technical training for its staff. Security reminders should be circulated among all staff on a regular basis. All personnel involved with personal data should be fully aware of and adequately trained in the service operator's security and privacy protection practices and procedures.

Directory Enquiry Service

24. A service operator which provides fixed telecommunication network

services is required to provide telephone directory service in relation to all their customers, other than those who have requested their information not be disclosed (i.e. ex-directory service). A service operator should prepare clear operational guidelines for its operators to follow in answering enquiries relating to ex-directory service customers and ensure no information of these customers are disclosed by operators.

Staff Deployment

25. When selecting staff to fill critical positions in which they will have access to sensitive customer personal data in carrying out their daily duties, a service operator should consider staff integrity as one of the selection criteria.

Supervision

26. Routine and random supervisory checks are effective tools to early detection of unexpected/irregular activities of employees, e.g. system access during odd hours or unusually high levels of system access. Supervisors should also closely monitor activities of staff who are assigned to perform high risk tasks in order to early detect possible abuse of authorities e.g. bulk printing of customer information or down loading of customer personal data.

E. Transfer of Customer Personal Data

27. A service operator may engage third party contractors or agencies for the provision of service including but not limited to conduct installation and repair work on its behalf for customers and for the purpose of collecting overdue charges from its customer in case of debt collection. In this connection, it may have to transfer the necessary customer personal data to these outside parties. It is understood that the service operator should bear the responsibility for infringing act of the outside party. In such cases, a service operator:

(a) should inform the customers on or before collection of the data concerned that the data may be transferred to such classes of persons;

(b) should transfer only such data relating to the customer concerned as are necessary for the outside parties to carry out the activity concerned;

(c) should take all practicable steps to ensure that customer personal data are

transferred to outside parties in a secure manner;

(d) should include terms and conditions in the agreements signed between the service operator and the outside parties to :

(i) prohibit the outside parties as well as their employees from divulging customer personal data obtained in the course of their duties;

(ii) oblige the outside parties to protect these customer personal data by complying with the data protection principles and policy to the same standard as the service operators required in Hong Kong;

(iii) require the outside parties to return or destroy all customer personal data transferred to them if these data are no longer required;

(iv) Require the outside parties to provide an audit report on compliance to the requirements when necessary; and

(v) make a declaration that customer personal data transferred to them are not copied or used for purposes other than those assigned; and

(e) should take all practicable steps to ensure the outside parties comply with these terms and conditions of the agreement.

Security Review and Audits

28. Owing to the ever changing business environment and technological developments, the effectiveness of security measures imposed may weaken as time goes by. A service operator should review the security of the systems from time to time to evaluate and assess their practical effectiveness, and to identify new corruption prone areas for necessary remedial actions. The opportunity should also be taken to identify instances of non-compliance with existing policies and procedures.

Enforcement

29. The Code is voluntary in nature. Fixed and mobile service operators are to self-police the compliance with this Code. Each member has the responsibility to maintain both integrity and goodwill of the telecommunications industry.

Consumer Council
Independent Commission Against Corruption
Office of the Privacy Commissioner for Personal Data
Office of the Telecommunications Authority

17 June 2002