CANADIAN AND JAPANESE BANKS ADOPT PRIVACY CODES

Respect for the privacy of financial data is a claim made by banks and other financial institutions by tradition and good business practice. Yet data protection authorities receive a high proportion of complaints about financial records. How should data protection be regulated in those countries without private sector privacy laws?

The OECD's approach is to encourage business sectors in member states without comprehensive data protection laws to draw up their own codes of practice to demonstrate that self-regulation can be equivalent to national law. The OECD's Paris meeting in May reviewed two of the most recent codes in the banking sector: those of the Canadian Bankers' Association, issued on 12th June last year, and Japan's Centre for Financial Industry Information Systems, published in March this year. This report covers both codes and illustrates the difficulties of a sector accustomed to defining its own standards of business confidentiality adjusting to a new era of external data protection regulation.

Both codes were drawn up to demonstrate that privacy laws are not needed for the banking sector in these countries. Both acknowledge data subjects' rights but carefully balance them against a strong assertion of traditional bank rights. But both codes share common weaknesses of having no enforcement provisions, nor a mechanism for referring dissatisfied data subjects to an independent ombudsman or arbitrator.

There are differences between them. The Japanese code takes the conventional approach of stating what banks should do, while the language of the Canadian code suggests that all provisions are a statement of practice. The Canadian Code covers customer data only, and is therefore aimed at satisfying customer concerns, while the Japanese code defines personal data more broadly, which relates to employees, suppliers and any other name-linked records.

The following report summarises the two codes without further comment.

The Model Privacy Code of the Canadian Bankers' Association

1. Introduction

The introduction states that the model code builds on the Canadian banks' tradition of "maintaining accuracy, confidentiality, security and privacy of customer information." It also supports the OECD Guidelines. The code covers the procedures by which personal information should be collected, stored, disclosed to third parties, verified and corrected, and serves as a model for individual banks to develop their own policies on privacy.

2. Application

The code applies to:

1. "all personal information, not just financial information, acquired as

a result of banking relationships or provision of services to an individual."

2. "all controlled operations of Canadian banks, both domestic and international, subject to any limitations or restrictions imposed by applicable local law."

Personal information is defined in the code as "factual information identifying and relating to a specific individual." Banks expect their outside suppliers to treat personal information in a confidential manner.

3. Collection of Personal Information

"Banks collect only enough personal information about their customers for the purposes of establishing and maintaining a banking relationship, providing specific services, rendering credit decisions, protecting the customers' and the banks' interests, marketing services, and complying with the law."

"At or before the time of collection, banks tell their customers how the information will be used and obtain consent to verify and supplement the information with external sources. These are principally credit sources, income sources and personal references. A record is kept of these external sources. The banks collect information only by lawful means."

4. Subsequent Use by the Bank and Disclosure to Third Parties of Personal Information

Personal information is used only for the purposes for which it is collected. But there are four circumstances under which disclosure of personal information may be made to third parties, "as dictated by prudent bank practice and/or legal requirements:

1. Customer consent

2. Legal obligations - The banks protect the interests of their customers by ensuring that:

a) "customers may be notified at their usual address/telephone numbers that an order has been received where this is not prohibited by law or where the customer is entitled by law to receive such notice from the bank,

b) orders appear to comply with the laws under which they are issued, and

c) only the personal information legally required and no more is produced."

3. Banks' Interests: "There are instances where, in the legal interest of the banks, it is necessary to disclose customers' personal information. For example, when cheques are returned NSF (not sufficient funds), information specific to customers' accounts is revealed."

4. Public Duty: "In exceptional circumstances, banks may be under a public

duty to disclose personal information to appropriate authorities in matters of significant public interest."

"A record is kept of each time personal information is disclosed, including the nature of the disclosure, the date and the identity of the party to whom disclosure was made."

5. Verification and Accuracy of Information

"Customers may have access to personal information concerning them extracted from bank records by following procedures established by their bank. The banks will provide the information in understandable form within a reasonable period of time and at a reasonable cost."

"Incorrect or incomplete information will be amended and any difference of opinion as to correctness or completeness will be noted in the file."

"If erroneous personal information is disclosed by the banks to third parties and customers' interests could be harmed as may reasonably be determined by the banks, the banks will, wherever possible, take reasonable steps to convey corrections to those third parties."

6. Security

"Security measures are taken by the banks to protect against unauthorized access by third parties to customers' personal information, and to protect against alteration, destruction and disclosure of such information."

7. Responsibility for Privacy Protection

"Ultimate responsibility for privacy protection rests with the banks' senior management."

"All employees are required to conduct the business of the bank by which they are employed in accordance with their bank's privacy protection procedures."

"Customers are encouraged to discuss any privacy concerns directly with their bank."

Guidelines on the Protection of Personal Data for Financial Institutions of The Centre for Financial Industry Information Systems (FISC), Tokyo

This is a voluntary set of guidelines, based on the OECD Guidelines, and drawn up by FISC's Expert Committee on Personal Data Protection which consist of academics and FISC members. The members include banks, insurance companies, securities companies, and credit card companies. These institutions state that they intend to handle personal data in accordance with these guidelines.

The guidelines cover automated personal data, defined as "any information relating to an identified or identifiable individual."

1. Collection of Personal Data

"The collection of personal data should be limited to the extent necessary to conduct business as specified under laws and regulations concerning financial institutions."

"Personal data should be obtained by lawful and fair means."

"In collecting personal data from a third party, financial institutions should strive to avoid imparting unwarranted harm to any interests of the data subject worthy of protection."

2. Use and Disclosure of Personal Data

"Use of personal data in financial institutions should, in principle, be limited to the confines of business specified by laws and regulations concerning financial institutions."

"Disclosure of personal data to third parties should be limited to those cases where:

a) the disclosure is within the confines of business specified by laws and regulations concerning financial institutions, or is requested to ensure justifiable interests of the data recipients, and is not likely to damage justifiable interests of the data subject worthy of protection; or

b) the data subject consents to disclose the personal data to third parties; or

c) the requests for the disclosure are made for the public interest, including requests under laws and regulations."

The code has official comments which elaborate on each point in the code. For example, the comment on a) above explains that financial institutions are able to disclose personal data to third parties "when the disclosure ensures socially justifiable interests of data recipients, for instance, minimizing business risks, and is not likely to harm justifiable interests of the data subject worthy of protection." The comment continues that the disclosure should be made carefully, for instance, only when the protection of personal data is assured after it has been released.

The code recognizes different rules for different circumstances, for example, regarding credit information. "The consent of the data subject is required in advance for the disclosure of personal credit information to a credit bureau, mainly because of the greater possibility of the data being widely used in the financial system."

3. Proper Management of Personal Data

"Personal data should be kept accurate to the extent necessary for their proposed use. The period of time that personal data is to be stored on file should, in principle, be specified."

"Personal data should be protected by reasonable security safeguards against such risks as unauthorized access, loss, destruction, modification, leakage, etc."

"In the event that the processing of personal data is entrusted to a third party, terms should be provided in the contract with regard to maintenance and management of data including keeping confidentiality."

4. Individual Participation

"Requests by the data subject backed by identification to gain access to his personal data should be accepted as far as possible, except in cases where it is considered inappropriate to inform the subject of the content in the light of customary practices etc."

"Requests to correct errors in personal data should be accepted without delay."

The commentary expands on when it would be "inappropriate" to disclose all of individuals' records to them. "In light of the privacy of the general public and customary practices, it is reasonable to withhold certain data such as individual evaluation and medical history, which are not supposed to be disclosed to the data subject. In addition, replying uniformly to all data requests would interrupt operations at financial institutions. Unspecified requests, requests for a means of collecting data and the records of data use and disclosure etc. are considered unacceptable."

The commentary concludes with a statement on access charges. "Financial institutions may impose a reasonable charge on a person who requests data disclosure unless the request is to amend inaccurate data."