

World Data Protection Report

International Information for International Businesses

Monthly news and analysis of data protection and privacy issues from around the world

Japan: Personal information privacy update

*By Jay Ponazecki, Daniel Levison, Toshihiro So
Morrison & Foerster, Tokyo*

*This article has been published in the December 2007 issue of
BNAI's World Data Protection Report*



www.bnai.com

Japan

Personal information privacy update

By Jay Ponazecki, Daniel Levison, Toshihiro So. Ms. Ponazecki is a partner in Morrison & Foerster's Tokyo business department. Mr. Levison is an associate in Morrison & Foerster's Tokyo litigation department. Mr. So is an associate in Ito & Mitomi, registered associated offices with Morrison & Foerster. Ms. Ponazecki, Mr. Levison and Mr. So are members of the firm's privacy practice group, which advises clients on a variety of privacy and data protection issues, including compliance with Japan's privacy-related laws and guidelines.

Morrison & Foerster LLP, Shin-Marunouchi Building 29th Floor, 5-1, Marunouchi 1-chome, Chiyoda-ku, Tokyo 100-6529, Japan. +81-3-3214-6522

Japan's Law Concerning the Protection of Personal Information (the "Law") came into effect for private sector businesses in April 2005. The Law provides only a broad outline for the Japanese privacy regime, the details of which are left to various government ministries to regulate through a patchwork of guidelines and other administrative guidance. Over the last two and a half years the ministries have developed new guidelines and amended existing ones.

The activities of a majority of businesses are covered by the guidelines promulgated by at least one of the following agencies: the Ministry of Economy, Trade and Industry (METI), the Ministry of Health, Labour and Welfare (MHLW), the Financial Services Agency (FSA), the Ministry of Internal Affairs and Communications (MIC), and the Ministry of Land, Infrastructure and Transport (MLIT). However, as of September 1, 2007, there are as many as 35 sets of guidelines issued pursuant to the Law, covering 22 business areas, including two sets of newly published guidelines and five sets of revised guidelines in the fiscal year 2006.

In general, the Law requires businesses to state the purpose of use of personal information at the time of collection, and prohibits use beyond that stated purpose. Subject to certain exceptions, the Law also generally prohibits disclosure of personal data to third parties without consent. Corporate subsidiaries and affiliates are considered third parties for the purposes of the Law. The Law also requires that businesses acquire personal information fairly, maintain accurate data, adopt security control measures, supervise employees and delegates (such as data processors and payroll or direct marketing vendors), permit access and correction of personal data, and create a system to address complaints regarding the handling of personal information. The details of these requirements are set out in the ministerial guidelines.

The definition of personal information

The definition of personal information under the Law is very broad, and includes any information specifically identifying a living individual, even information that is not related to what one might normally consider information of a personal or private nature (e.g., personnel records, financial information, medical information, etc.) may fall under this definition. There

is no exception for information used by an individual in his or her business or professional capacity. Therefore, personal data includes, for example, publicly available information and business contacts, such as records in an electronic address book, business cards in a file, marketing lists, and email messages displaying names and email addresses. Recorded images in which a specific individual can be identified are also considered personal data. Companies that hold personal data relating to 5,000 people or less and ordinary private use of personal information are exempted from the requirements of the Law.

Recent trends

Because of the breadth of the definition of personal information and the wide reach of the Law and its related guidelines, there has been significant discussion and debate regarding the interpretation and enforcement of this regulatory framework.

The Quality of Life Council of the Japanese Cabinet Office started a review of the Japanese government's activities relating to the protection of personal information in November 2005 and a summary of the Quality of Life Council's findings was submitted to the government in June 2007. In September 2007, the Cabinet Office issued a report on the status of enforcement of the Law.

Public perception of the Law

As part of this process, the Cabinet Office identified a growing number of incidents of "overreaction", situations in which misunderstandings about the applicability of the Law caused personal information to be withheld inappropriately. For example, schools and resident associations stopped creating and distributing emergency contact lists, police and other law enforcement officials were refused lawful requests for information during investigations, and social workers were refused personal information necessary for conducting their duties relating to the care of children and the elderly. To prevent such "overreaction," the Japanese government is undergoing a campaign to educate the public further about the applicability of the Law and establishing hotlines and dedicated emailboxes to respond to questions from the public. The Cabinet Office, in co-operation with the relevant ministries, also plans to develop best practices to assist the public in better understanding of the Law.

Recent trends in enforcement

As part of its review, the Cabinet Office also released statistics regarding the enforcement of the Law. The overall number of cases in which the ministries required self-reporting decreased in fiscal year 2006, while the number of recommendations issued by the ministries rose from one case to four. Of those four cases, two related to data leaks arising from insufficient security controls or supervision of employees and vendors and two related to improper use of personal information beyond the purpose of use stated at the time of initial collection, as

well as to insufficient security controls or supervision of employees and vendors.

It makes sense that, of the cases in which public bodies were consulted, a significant number of complaints related to the improper acquisition of personal information. However, while data leaks continue to be high profile news items, they accounted for less than 25 of public consultations. Of these consultations, most leaks related to consumer information and, of those leaks, information beyond mere names, dates of birth and addresses was leaked. The leaked information included telephone numbers, account numbers, credit card numbers, and email addresses. More than 75 of the leaks, however, were on a relatively small scale, involving the personal information of less than 500 individuals. Of leaks experienced by businesses, most leaks caused by employees were accidental, while leaks caused by third parties tended to be intentional, such as theft of the personal information. More than 90 of leaks resulted in businesses instituting better security control measures.

While there have not been significant administrative fines or penalties or court judgments arising from failures to comply with the Law and the related guidelines, the risk of damage to businesses is still great. Recent trends show an increasing public sensitivity towards the use and misuse of personal information. In fact, nearly 70 of survey respondents agreed with the statement that their personal information is being used in ways that they did not anticipate.

The mishandling of personal information can cause significant, and often underestimated, damage to public trust and goodwill. While it may be nearly impossible to completely eliminate the risk of a data leak, prevention is still the best way to minimise the risk. Businesses should regularly review their current practices regarding the collection, use and transfer of personal information, and identify ways to improve such practices, especially regarding the transfer of data to third parties and the handling of data by vendors and other delegates.