Global Privacy - Japan Sets its Rules for Personal Data

Global companies must comply with differing privacy rules. The great divide between the EU and the USA is well-known. The EU is an “opt-in” system, insisting generally on express agreement by individuals before a company can share or use their personal data. By contrast, the USA is largely an “opt-out” regime, using a mix of sector-specific rules plus public declaration. In some areas in the US, express opt-in is required (e.g., medical records), in others privacy notices about company rules are sufficient, and in yet other areas the rules are not clear or are flexible. Canada follows a third approach.

Japan’s Law Concerning the Protection of Personal Information (“Privacy Law”) took effect April 1, 2005. Japan’s approach is in some respects more stringent than the EU standard, and more difficult to apply than the US or Canadian rules. Immediate attention should be given to the Japanese requirements by any large company that gathers, maintains or uses personal data about Japanese nationals. Smaller companies may be exempt from the Privacy Law, as discussed below.

Japan relies on a detailed regulatory framework plus private sector self-regulation. The Japanese Privacy Law is similar to the EU Directive, in the sense that it establishes a required framework for Japan’s ministries to implement through detailed regulations in all sectors of Japanese life. The Prime Minister issued a Basic Policy in April 2004, which a year later became the basis for Japan’s Privacy Law. Different ministries developed specific regulations that conform to the Basic Policy, and now to the Privacy Law. For example, the Ministry of Justice issued regulations regarding personal data involved in loan servicing and universities, and the Ministry of Internal Affairs and Communications issued the rules affecting telecommunications and broadcasting.

Handling of Personal Information in Japan

The Privacy Law defines “personal information” very broadly. It covers all the data or all living persons that “can be used to identify specific individuals by name, date of birth, or other description.” It includes publicly available information (phone numbers) as well as business contacts, HR data and patient records. It is hard to think of facts about a person that do not qualify as “personal information.”
Global Privacy - Japan Sets its Rules for Personal Data

Businesses that use personal information have specific prescribed duties as to personal information. Virtually any business with a Personal Information Database is covered, as long as at least 5,000 individuals are in the database. A company database involving fewer than 5,000 people is exempt from the Privacy Law, based on a government ordinance declaring that such a limited database is not a threat to individual rights. Smaller businesses, however, should consider conforming to the basic rules affecting their industry, or run the risk of failed employee expectations or worse.

Businesses with Personal Information Databases of more than 5,000 people must take the following steps:

1. Specify the purposes for which personal information will be used;
2. Restrict usage to necessary measures;
3. Obtain the information in a fair manner;
4. Provide notice to persons about the reasons for use, and obtain consent before sharing information with third parties;
5. Keep data secure, including adoption of security control measures;
6. Carry out effective supervision of those who handle personal information;
7. Allow persons to access and revise information about them; and
8. Have a complaint handling system.

Individuals must be told why and how their personal data will be used. This can be done by notice, without specific opt-in (e.g., by website or letter). The form of notice differs depending on the situation. Employees, for example, must be told in detail enough information so that they can understand the ultimate uses of their data. Financial Services Agency (FSA) regulations require businesses to identify by name those third parties that might receive information (generic description is insufficient). For each particular type of intended use, applicable Ministry regulations must be followed to design the notice properly.

If the purpose of stated usage changes (e.g., an employer decides after the initial notice that it will provide personal information for the purpose of setting up a 401(k) plan to a third party administrator), a new notice must be sent. The level of detail for notices goes beyond EU and US requirements. Thus, Japanese privacy notices will require more detailed drafting, and probably more updating, than is the case outside Japan.

Third Party Disclosures
Third party disclosure follows an opt-in regime, like Europe and unlike the US. Affiliates of companies are considered third parties. Thus, if a Japanese subsidiary of a US company wants to send home addresses of Japanese employees to the US parent (so that holiday cards might be sent from the US CEO), this requires advance permission of the Japanese individuals. The originating business, under several ministry regimes, will remain accountable for what third parties do with the data. As a result, the sending business must obtain assurances from third parties regarding proper use and restrictions regarding the data to be shared.
There is a joint use exception that allows sharing of personal information with third parties without express consent, but this depends on obtaining individuals’ express agreement to this at the time the privacy notice is sent to the individuals with a clear description that joint use is intended. The joint use must be stated in a detailed manner for it to be lawful later.

For some uses, an opt-out exception is provided for the sharing of personal data. Most businesses may share data without an express opt-in by an individual if they have provided prior notice to the person that (1) use of the data includes providing information to specified third parties; (2) specific information can be shared with third parties; (3) transfer of the data will occur by specified methods; and (4) the individual may stop transfer upon request. Financial services businesses cannot use the opt-out exception, and are instead required to get express agreement from individuals before sharing personal data, even with affiliates.

Other Requirements Under Privacy Law
Financial services businesses face other requirements, including appointment of a Chief Privacy Officer, internal inspection and external audits and specific ledger books about protection and use of personal data. By contrast, the Ministry of Economy, Trade and Industry Guidelines provide standards for security controls, leaving the specific method of achieving them to affected businesses (e.g., consumer credit companies). In general, Japan’s Privacy Law requires more specific and detailed measures for data security than are present in other countries.

Japan’s Privacy Law requires that individuals have access to personal information kept about them and that businesses respond promptly to access requests, with limited exceptions. If a person looks at data and demands a correction, the business is required to make a proper correction and notify the person of action taken (including why a request was denied).

Unlike European countries, Japan does not have specific rules about moving personal data outside of Japan. This is because Japan makes no distinction between moving data to third parties inside or outside of Japan. In either case, third-party disclosure and joint use rules apply.

The Privacy Law is not optional. It is backed by the potential of large fines and up to six months imprisonment, not to mention adverse publicity that surrounds failures in the handling of personal data.

Compliance with Japan’s Privacy Law must be part of a global strategy for data handling. Measures will vary depending on the nature of the business and personal data information involved. Affected businesses should be clear about the particular guidelines or rules that govern them and devise a system to meet the requirements. After that, ongoing steps must be taken to ensure the system works as designed. These measures should address what happens in the event of a breach of the privacy program that is established.