

Japan's Personal Information Protection Act

2003 Law No. 57

Passed 2003; in force as to companies (non-government) since April 1, 2005

Translation of Provisions Relevant to Business (i.e., Chapters 1, 3-6)

This is an unofficial "reading" translation edited for clarity over word-for-word correspondence with the Japanese text.

This is not a literal transcription.

Only the Japanese text is official.

translation © 2005 Proskauer Rose LLP
All rights reserved

Permission to quote from or reproduce this copyrighted translation is
granted only if expressly attributed to:
"Proskauer Rose LLP © 2005 unofficial translation."

Proskauer Rose LLP offers practice areas in, among others,
Privacy and International Employment Law.
Visit www.Proskauer.com.

Chapter 1 General Provisions

Section 1 Purpose

This law was passed because of the spread of personal information in our advanced-information/telecommunication society. The law tries to protect individuals' rights and welfare while preserving the usefulness of personal information. The intent is to set out a policy for handling personal information, and measures for protecting personal information. This law spells out duties of the national and local government. It also sets out obligations of businesses that handle personal information.

Section 2 Definitions

1. “Personal Information” means information relating to living individuals which identify specific individuals by: name, date of birth, or other description (or which, when easily compared with other information, can identify specific individuals).
2. “Personal Information Database” means a collection of information, including Personal Information, which is:
 - i. Structured so as to be easily-retrievable, by specific Personal Information, by computer; and
 - ii. Designated by government ordinance as structured so as to be easily-retrievable, by specific Personal Information.
3. In this law, “Business” means a person or entity that uses Personal Information Databases for business operations, but excludes:
 - i. Organs of the national government;
 - ii. Local public entities;
 - iii. Independent administrative corporations defined in the “Law on Protection of Personal Information Held by Independent Administrative Corporations” (2003 Law No. 59), section 2 ¶ 1;
 - iv. Local independent administrative corporations as defined in the “Local Independent Administrative Corporations Law” (2003 Law No. 118), section 2, ¶ 1;
 - v. Persons or entities which a government ordinance designates as posing little or no threat to individuals’ rights or welfare, because of the quantity of Personal Information they use and how they use it.

Editor’s note: To implement section 2 ¶ 3(v), above, the Japanese government issued an ordinance/cabinet order on December 10, 2003:

Government Ordinance of Personal Information Protection Act (December 10, 2003; Government Ordinance No. 507), section 2:

“Persons or entities which a government ordinance designates,” as used in section 2 ¶ 3(v) of the Personal Information Protection Act, includes any entity which—on any day in the past six months—maintained (and used in its [presumably worldwide] business operations) databases containing information on less than 5000 total specific identifiable individuals. In counting the 5000, you can exclude names in databases created by another entity and not further processed, if those database limit data to these three categories: name; address/domicile; business telephone number.

4. “Personal Data” means Personal Information which makes up a Personal Information Database.

5. “Preserved Personal Data” means Personal Data which a Business has authority to: disclose, correct, add to, delete, stop using, eliminate, or stop providing to third parties—other than information which some government ordinance designates as information which, if disclosed, would threaten public (or other) welfare, and other than information which some government ordinance requires eliminating within a year or less.

6. “Principal” (as used with respect to Personal Information) means a specific individual identified by Personal Information.

Section 3 Philosophy

Respect for the individual requires treating Personal Information carefully. So treat Personal Information appropriately.

Chapter 2 Duties of National Government and Local Public Entities, Etc.

(This chapter does not relate to businesses.)

Chapter 3 Measures for the Protection of Personal Information

(Notwithstanding the title, this chapter relates only to government entities—not businesses.)

Chapter 4 Duties of Businesses

Subchapter 1. Duties of Business

Section 15 Specifying “Purpose of Use”

1. As possible, a Business must articulate its *Purpose of Use* for processing Personal Information (hereinafter “Purpose of Use”).
2. No Business may change its Purpose of Use, unless the change stays reasonably within the scope of its original Purpose of Use.

Section 16 Limits on “Purpose of Use”

1. No Business may process Personal Information beyond its stated Purpose of Use—unless the Principals consent beforehand.
2. No Business that gets Personal Information as a successor to some other Business’s operations (such as by merger) may handle that Personal Information beyond its Purpose of Use articulated before the succession—unless the Principals consent beforehand.

3. The above two paragraphs do not apply where the processing:
 - i. Is pursuant to a law or ordinance;
 - ii. Is necessary to protect human life, safety, or property—and when it is difficult to get the Principal’s consent;
 - iii. Is necessary to improve public hygiene or promote childrens’ health—and when it is difficult to get the Principal’s consent;
 - iv. Would require taking some act required by some law or ordinance—and where taking that act could be hindered by having to get the Principal’s consent.

Section 17 Acquiring Personal Information

A Business shall not get Personal Information unfairly or by fraud.

Section 18 Notification of Purpose of Use in Acquisition

1. Upon receiving Personal Information, a Business must promptly tell the Principal (or publicly announce) its Purpose of Use—unless its Purpose of Use had already been publicly announced.
2. Notwithstanding paragraph 1, if a Business receives a Principal’s Personal Information through some contract (or document executed with a contract) with that Principal—including electronic/magnetic or other documents not in hard copy, or if a Business acquires the Personal Information of a Principal via some document from that Principal, then the Business must disclose (in advance) its Purpose of Use to the Principal, unless some urgent need for the protection of human life, safety, or property prevents doing so.
3. A Business that changes its Purpose of Use must either notify affected Principals or publicly announce its new Purpose of Use.
4. Paragraphs 1-3 do not apply if:
 - i. Life, safety, property, or other right (or the welfare) of the Principal (or a third party) could be harmed by notifying the Principal of, or publicly announcing, the Purpose of Use;
 - ii. Rights or profits of the Business could be harmed by notifying the Principal of, or publicly announcing, the Purpose of Use;
 - iii. Compliance with some law or ordinance could be compromised by notifying the Principal of, or publicly announcing, the Purpose of Use;
 - iv. The Purpose of Use is obvious from the very way the Business got the Personal Information.

Section 19 Accuracy of Data

A Business must diligently maintain Personal Data as accurately and up-to-date as necessary to achieve its Purpose of Use.

Section 20 Security Control Measures

A Business must take steps to prevent the unauthorized disclosure, loss or destruction of Personal Data. And it must protect Personal Data security.

Section 21 Supervision of Employees

To protect data security, a Business must supervise employees who handle Personal Data.

Section 22 Supervision of Delegates

To protect data security, a Business must supervise anyone to whom it delegates handling its Personal Data.

Section 23 Restrictions on Providing Data to Third Parties

1. A Business shall not give Personal Data to any third party, without first getting the Principal's consent, unless:

- i. Pursuant to a law or ordinance;
- ii. Necessary to protect human life, safety, or property—and when getting the Principal's consent is difficult;
- iii. Necessary to improve public hygiene or to promote childrens' health—and when getting the Principal's consent is difficult;
- iv. Some law or ordinance requires the Business to do something—and having to get the Principal's consent would hinder the Business's compliance.

2. Principals have a right to tell Businesses not to transfer their information on to third parties. Businesses have to tell Principals they have this right. Where a Principal does *not* exercise this right, the Business *can* transfer that Principal's data to third parties, but only if the business first notifies the Principal (or the Principal can easily learn):

- i. That giving the Personal Data to a third party is within the Business's Purpose of Use;
- ii. What categories of Personal Data the Business is giving the third party;
- iii. How the Business gives Personal Data to the third party;
- iv. That the Business will stop giving the third party the data if the Principal requests.

3. If a Business changes the categories of Personal Data it gives third parties, or if it changes how it gives Personal Data to third parties, that Business must first notify the Principal of these changes—unless the Principal can easily learn them.

4. Any party who has received Personal Data shall *not* be considered a “third party” under ¶¶ 1-3, if:

- i. The Business delegates some or all of the Personal Data handling to that party, in order to achieve its Purpose of Use;
- ii. The transfer of Personal Data to that party is part of a succession of business operations (such as a merger);
- iii. The Business and that party jointly use the Personal Data, and the Principal got notice about (or can easily learn of) the joint use—and where that notice also communicated: what Personal Data would be used jointly; who the jointly-using parties are; what the joint parties’ Purpose of Use is; and the name (or title) of the joint parties’ contact person.

5. As to paragraph 4(iii), if a Business changes its Purpose of Use, or if the name or title of the person responsible for managing Personal Data changes, then the Business must notify the Principal in advance (unless the Principal can easily learn of the changes).

Section 24 Public Announcements Relating to Preserved Personal Data

1. A Business must ensure that Principals can easily learn of, and must promptly respond to Principals’ inquiries regarding, the following, as to Preserved Personal Data:

- i. Name of the Business;
- ii. The Business’s Purpose of Use of all Preserved Personal Data (except for data subject to section 18 ¶4 (i)–(iii));
- iii. The Business’s procedures for responding to requests under section 24 ¶¶ 1, 2; section 25 ¶1; section 26 ¶1; section 27 ¶2—including the cost of any processing fees imposed under section 30 ¶2;
- iv. Matters which some government ordinance says are necessary for special handling of Preserved Personal Data.

2. If a Principal asks a Business for information about his Preserved Personal Data, the Business has to give it to him promptly—except:

- i. Where the Purpose of Use is already clear; or
- ii. In any case falling under section 18 ¶1(i)–(iv).

3. A Business that refuses to comply with a request under paragraph 1 must promptly notify the Principal of its refusal.

Section 25 Disclosure

1. If a Principal asks a Business to disclose his Preserved Personal Data, the Business must promptly disclose it (or disclose that none exists, if that is the case), using a disclosure method set out in a government ordinance. However, the Business may refuse to disclose all or some data, if disclosure would:

- i. Endanger life, safety, property, or welfare of the Principal or a third party;
- ii. Significantly impair the Business's operations;
- iii. Violate some law or ordinance.

2. A Business that refuses to comply with a request under paragraph 1 must promptly notify the Principal of its decision.

3. If some law or ordinance imposes some method for disclosing Preserved Personal Data, then that law or ordinance shall control over paragraph 1.

Section 26 Corrections

1. If a Principal asks a Business to correct, supplement, or delete any of his Preserved Personal Data because he claims the data are incorrect, the Business must investigate the claim, and, if circumstances warrant, correct—unless some law or ordinance imposes other procedures.

2. A Business must promptly notify a Principal after it corrects or deletes any Preserved Personal Data under paragraph 1 (or after it decides not to correct or delete).

Section 27 Cease Use

1. If a Principal asks a Business to stop using (or to delete) any of his Preserved Personal Data on the grounds that the Business violated sections 16 or 17—and if the Business finds this claim has merit—the Business must promptly stop using (or delete) the data, as necessary to correct the violation. However, the Business may reject the request, if complying would be very expensive or difficult—but in that case, the Business has to take steps to protect the Principal.

2. If a Principal asks a Business to stop giving his Preserved Personal Data to some third party, claiming a violation of section 23 ¶1—and if it is clear that grounds exist—then the Business must stop promptly. However, the Business need not stop if complying would be very expensive or difficult—but in that case, the Business has to take appropriate steps to protect the Principal.

3. A Business must promptly tell a Principal what steps or decisions it takes under paragraphs 1 and 2.

Section 28 Explanation of Reasons

If (under sections 24 ¶3; 25 ¶2; 26 ¶2, or 27 ¶3) a Business tells a Principal it refuses to do what he asks—or if a Business tells a Principal it will take steps different from what he wanted—then the Business must try to explain to the Principal what it is doing, and why.

Section 29 Procedures for Responding to Request for Disclosure

1. A Business may set up its own procedures for answering requests under sections 24 ¶2; 25 ¶1; 26 ¶1; or 27 ¶¶1-2, as long as those steps are consistent with any ordinances. If a Business lays out procedures, Principals have to follow them.
2. If a Principal makes a request, a Business can force the Principal to tell the Business anything it might need to know to comply with that request. But the Business must facilitate the Principal's easy and accurate compliance.
3. Consistent with ordinances, any request can come from someone's agent or attorney.
4. In responding to Principals' requests, Businesses may not impose excessive burdens.

Section 30 Processing Fees

1. A Business replying to a Principal's request under sections 24 ¶2 or 25 ¶1 can charge a processing fee.
2. Any fee set must be reasonable in light of the Business's actual expenses.

Section 31 Processing of Grievances by Business

1. A Business must use best efforts promptly to process grievances that involve handling Personal Information.
2. A Business must use best efforts to establish a grievance resolution system.

Section 32 Collection of Reports

The State Minister in Charge (as necessary to enforce this subchapter) may force Businesses to tell how they handle Personal Information.

Section 33 Advice

The State Minister in Charge (as necessary to enforce this Subchapter) may advise Businesses how to handle Personal Information.

Section 34 Admonishments and Orders

1. If necessary to protect individuals, if the State Minister in Charge finds a Business violated sections 16 - 18, 20 - 27, or 30 ¶2, the Minister may tell the Business to stop violating the law—or to do something else.

2. If the State Minister in Charge finds some important individual right is imminently threatened by a potential violation of this law—and if the affected Business has been warned (under paragraph 1) but persists in violating the law—the Minister may order the Business to take appropriate steps.

3. If the State Minister in Charge finds some Business violated sections 16, 17, 20-22, or 23 ¶1 and in doing so deprived someone of some important right, and if the Minister decides it is urgently necessary to fix the problem, then the Minister may order the Business to stop violating the law—or to correct its violation.

Section 35 Limits on Exercising State Minister in Charge’s Authority

1. In taking steps under sections 32 - 34, the State Minister in Charge has to respect peoples’ freedom of expression, academic freedom, freedom of religion and freedom of political activity.

2. The State Minister in Charge shall not take steps under sections 32-34 if the exclusions in section 50 ¶1 apply.

Section 36 State Minister in Charge

1. The Prime Minister may (if he finds it necessary) appoint a minister or a National Public Safety Committee as State Minister in Charge of certain aspects of handling Personal Information. These State Ministers in Charge shall be:

- i. As to data about employment: the Minister of Health, Labor and Welfare, or (as to employment of seamen), the Minister of Land, Infrastructure and Transport;
- ii. As to other business data: the Minister with authority over the corresponding business sector.

2. The Prime Minister must publicly announce any State Minister in Charge appointed.

3. State Ministers in Charge must cooperate among themselves in enforcing this subchapter.

Subchapter 2. Promotion of the Protection of Personal Information by Private Organizations

Section 37 “Approved Personal Information Protection Organizations”

1. The State Minister in Charge may affirmatively appoint “Approved Personal Information Protection Organizations” to:

- i. Process grievances about Personal Information by a Business, under section 42;
- ii. Give a Business information that helps it handle Personal Information;
- iii. Handle Personal Information by a Business.

2. Anyone who seeks appointment under paragraph 1 must apply to the State Minister in Charge, consistent with governmental ordinances.
3. The State Minister in Charge must publicly announce any appointments.

Section 38 Conditions for Disqualification

The following may *not* be granted a section 37 ¶1 appointment:

- i. Anyone subject to criminal penalties under this law (unless the penalty ended over two years ago).
- ii. Anyone whose approval under this law was cancelled under section 48 ¶1 in the last two years.
- iii. Officers/agents/representatives/managers of any Business:
 - (a) Punished with at a penalty of imprisonment, or punished under this law, within the last two years;
 - (b) Cancelled under section 48 ¶1 in the last two years—if the individual served as officer/agent/representative/manager within 30 days before that cancellation.

Section 39 Standards for Approval

Those appointed under section 37 ¶1 must:

- i. have an infrastructure that operates appropriately and accurately.
- ii. have enough knowledge and ability—including accounting background—to operate appropriately and accurately.
- iii. be free of any conflicts from other activities (except for those set out in section 37 ¶1).

Section 40 Notification of Abandonment

1. If an appointee under section 37 ¶1 wants to abandon its approved operations, it must file a notice in advance with the appropriate State Minister in Charge.
2. The State Minister in Charge shall publicly announce any notice received under paragraph 1.

Section 41 Subject Business

1. Any appointee under section 37 ¶1 includes any organization that is a member of an appointee organization, or that has consented to being a member.

2. An appointee under section 37 ¶1 must publicly announce any member organizations under paragraph 1.

Section 42 Processing Grievances

1. When an appointee under section 37 ¶1 gets a grievance about handling Personal Information, it must: consult with the grievant; advise the grievant; investigate the grievance; tell the respondent what the grievance alleges; and seek to resolve the grievance promptly.

2. An appointee under section 37 ¶1 can request written or oral explanations of a grievance. It can also ask the respondent to submit materials.

3. If a respondent refuses a request from an appointee under section 37 ¶1, it needs reasonable grounds.

Section 43 Personal Information Protection Policy

1. An appointee under section 37 ¶1 shall try to draft (and shall publicly announce) a policy on: Purpose of Use, security, and procedures for responding to Principals' needs (a "Personal Information Policy").

2. After an appointee under section 37 ¶1 announces a Personal Information Policy, it must offer advice and take other steps to get Businesses to comply with it.

Section 44 Prohibition of Use for Improper Purposes

An appointee under section 37 ¶1 will use information it learns in the course of its business only within the scope of its business as appointee.

Section 45 Restrictions on Use of Title

Only appointees under section 37 ¶1 shall call themselves "Approved Personal Information Protection Organizations" (or something similar).

Section 46 Collection of Reports

The State Minister in Charge can force appointees under section 37 ¶1 to report on what they are doing, as necessary to enforce this law.

Section 47 Orders

The State Minister in Charge can force appointees under section 37 ¶1: to reform how they operate; to change their Personal Information protection policies; and to do anything else necessary under this law.

Section 48 Cancellation of Approval

1. The State Minister in Charge can cancel the appointment of an appointee under section 37 ¶1 if that appointee:

- i. Falls under section 38 ¶i or ¶iii,
- ii. Fails the tests under section 39,
- iii. Violates section 44,
- iv. Fails to obey an order under section 47, or
- v. Acquired its section 37 ¶1 approval unfairly.

2. The State Minister in Charge must publicly announce when it cancels approval.

Section 49 State Minister in Charge

1. When the Prime Minister finds it necessary, he may designate a specific Minister as the State Minister in Charge.

The State Minister in Charge of any given appointee under section 37 ¶1 is:

- i. the Minister that appointed that appointee, or, otherwise,
- ii. the State Minister in Charge with jurisdiction over the appointee's business sector.

2. When designating a State Minister in Charge, the Prime Minister must announce the designation to the public.

Chapter 5 Miscellaneous Provisions

Section 50 Exclusions

1. Chapter 4 does not apply to a Businesses where all—or a portion—of the reason it handles Personal Information is:

- i. *Reporting* (broadcast media, newspapers, news agencies, other reporting media, and including individual reporters by trade);
- ii. *Writing* (individuals who are writers by trade);
- iii. *Scholarly research* (universities and other organizations whose purpose is scholarly research, and individuals affiliated with them);
- iv. *Religion* (organizations whose purpose is religious activities);
- v. *Political* (organizations whose purpose is political activity).

2. “Reporting” means communicating objective fact as fact to an unspecified mass audience (including expressing thoughts and opinions based on the facts).

3. A Business covered under paragraph 1 must try to adopt: procedures appropriate and necessary to control Personal Data securely, and procedures necessary to process grievances related Personal Information. It must publicly disclose these procedures.

Section 51 Operations Performed by Local Public Entities

Governmental ordinances can allow the State Minister in Charge to delegate responsibilities to local public bodies and administrative agencies.

Section 52 Delegation of Authority and Operations

Governmental ordinances can allow the State Minister in Charge to delegate responsibilities to that Minister’s own agencies.

Section 53 Public Disclosure of State of Enforcement

The State Minister in Charge can force appointees under section 37 ¶1 to report on what they are doing, as necessary to enforce this law.

1. The Prime Minister can force “agencies” to report on what they are doing to enforce this law.

“Agencies,” in this sense, means:

- bodies designated under this law, except for the Cabinet Office
- agencies under the jurisdiction of the Cabinet, Cabinet Office, or Imperial Household Agency
- institutions designated under section 49 ¶1 and ¶2 of the Cabinet Office Establishment Law (1999 Law No. 89)
- institutions designated under section 3 ¶2 of the National Administrative Organization Law (1948 Law No. 120)).

2. The Prime Minister shall release a summary report under paragraph 1, every year.

Section 54 Contact and Cooperation

The Prime Minister and the heads of the administrative agencies responsible for enforcing this law must communicate and cooperate with each other.

Section 55 Delegation to Government Ordinance

The government shall issue ordinances to enforce this law.

Chapter 6 Penalty Provisions

Section 56

Anyone who violates an order under section 34 ¶¶2-3 can be put in prison for up to six months, or fined up to 300,000 yen.

Section 57

Anyone who fails to file a report under sections 32 or 46, or who files a false report, can be fined up to 300,000 yen.

Section 58

1. A *representative* can be punished under sections 56 and 57, as can any legal entity principal he represents.
2. A representative or manager must represent any institution not organized as a legal entity in civil and criminal proceedings.

Section 59

Anyone is subject to a fine of up to 100,000 yen if he:

- i. Failed to file a notice under section 40 ¶1, or files a false notice;
- ii. Violated section 45.

Supplementary Provisions

Section 1 Date of Enforcement

This law shall be enforced from the date it was promulgated. However, chapters 4 - 6 and Supplementary Provisions sections 2 - 6 shall be enforced only from the date determined by the governmental ordinances, which shall be within two years from promulgation.

Section 2 Transitional Measures concerning the Consent of Principals

If, before this law's effective enforcement date, some Principal had consented to any handling of Personal Information, that consent continues to be valid (as if under section 16 ¶¶1-2)—as long as the consent is equivalent to a consent under section 15 ¶1.

Section 3 Consent

If, before this law’s effective enforcement date, some Principal had consented to any handling of Personal Information, that consent is valid as if under section 23 ¶1—as long as the consent is equivalent to a consent under section 23 ¶1.

Section 4 Transitional Measures on Notice

If, before this law’s effective enforcement date, some Principal had given a notice (or circumstances arose in which notice could be easily learned) equivalent to notice under section 23 ¶2, then notice under that section is deemed made.

Section 5 Notice

If, before this law’s effective enforcement date, some Principal had given a notice (or circumstances arose in which notice could be easily learned) equivalent to notice under section 23 ¶4(iii), then notice under that section is deemed made.

Section 6 Transitional Grandfathering Use of Title

Anyone using the title “Approved Personal Information Protection Organization” (or something similar) before the effective enforcement date of this law will not be subject to section 45 until six months after it comes into effect.