



PERSONAL INFORMATION AUDIT CHECKLIST

The purpose of this Personal Information Audit (“PIA”) Checklist is to assist organizations in assessing current personal information handling practices.

The results from the PIA will be used to assess the level of privacy-related exposure of the business from a legal perspective and will be used to create an internal personal information policy for the organization. It is therefore important that the PIA be as thorough and complete as possible.

The PIA should also be conducted periodically, to ensure that the business has a current and accurate picture of the organization’s data flows, personal information handling practices and privacy compliance.

COLLECTION

The *Personal Information Protection and Electronic Documents Act* (“PIPEDA”) defines “personal information” as “**information about an identifiable individual**, but does not include the name, title or business address or telephone number of an employee of an organization”. Consider the above definition carefully when looking at the organization’s personal information collection practices.

1. From whom does the business collect personal information?

List all categories of individuals from whom the business collects personal information. For example:

- clients
- general public
- employees



2. What methods and/or technologies does the business use to collect personal information?

For each category above, set out the “collection points” for personal information. For example, for business members, the points of collection might include:

- standard forms
- point of sale
- surveys/questionnaires
- web site (e.g., cookies, online forms, log files, etc.)
- phone, fax or e-mail inquiries
- interviews
- chat rooms/online forums

3. What personal information is collected at each “collection point”?

List all personal information collected for that category of individual at a particular collection point. Considering the PIPEDA definition, personal information may include:

- name
- address
- credit card or other financial information
- birth date/age
- gender
- phone/fax numbers
- next of kin/emergency contacts
- marital status and other familial information (e.g., children, spouse, etc.)
- education details
- e-mail addresses, web site addresses, IP addresses for computers
- legal information (e.g., criminal record)
- employment/income details
- SIN number
- driver’s license information
- ethnicity
- membership status/results of investigations
- financial information
- medical history
- dialogue or interaction with an individual through correspondence, chat rooms, etc.
- other...



4. What personal information is being received from third parties?

Examples may include the following:

- marketing companies
- third party mailing lists
- other...

5. Would the individual know that a particular piece of personal information is being collected?

Consider whether the personal information was collected *passively* (i.e., without direct participation from the individual) or *actively* (e.g., by the individual filling out a form, giving consent, etc.)

6. What is the purpose of the information collected?

For each of the above, consider the purpose of collection and whether the collection of such personal information is reasonably necessary to carry on the business.

STORAGE AND MAINTENANCE

7. Where and how is personal information stored?

List all locations where personal information collected by the business is stored. For example:

- servers
- personal computers
- backed up computer files
- database management system
- hard copy (i.e., papers) files
- other...

Consider whether any of the above records are on-site, off-site and where that information is actually located.



8. What are the records retention and destruction practices of the business?

How long are records kept, and under what conditions are records containing personal information destroyed? Who is responsible or accountable for destruction of personal information?

ACCESS

9. Who within the business has access to personal information?

List the names and/or positions of all employees and other individuals who have general access to the various types of personal information collected.

Consider of these individuals, who actually *needs* to have access to this information.

10. Who outside of the business has access to personal information?

To what extent do individuals have access to his or her own personal information?

Also consider whether functions or activities involving personal information are contracted out to third parties (i.e., collection, storage). Examples include:

- copying services (i.e., photocopying, microfilming, etc.)
- web site hosting
- temporary or contract administrative replacements
- consultants
- computer technical help (including off-site electronic storage and backing up of files)

Of the above parties, consider how to minimize access to personal information.



11. Does the business have measures to protect the personal information it holds from unauthorized access?

For each method of storage, consider whether the business *has* or *needs to have* the following security measures in place:

- locked storage
- restricted access to computer system
- policies and procedures relating to data storage
- designated staff access to data
- training on access and security
- backing up of electronic files

Does the business have confidentiality/non-disclosure/personal information provisions in contracts with third parties, employees, etc.?

USE

12. How does the business use the personal information?

List all internal uses for personal information collected by the business.

Consider all primary and secondary uses for personal information collected. Secondary uses may include:

- marketing/research
- funding
- quality control
- other...

13. Does the business make individuals aware of all types of uses of personal information?

Consider whether individuals are made aware of the business' uses of personal information and whether the individual has consented to that use.



PATTERSON PALMER
Law

DISCLOSURE

- 14. Does the business give the personal information to anyone outside of the organization? To whom and where are these organizations located?**

Consider disclosures made to various governmental and non-governmental entities, including:

- government departments
- other potential employers
- lawyers
- insurance companies
- police
- credit agencies
- other...

- 15. Does the business make individuals aware of disclosures of personal information?**

Consider whether individuals are made aware of the business' disclosures of personal information and whether the individual has consented to that disclosure.

CURRENT PRACTICES

- 16. What are the business's current privacy policies and/or information handling policies?**

Append any current written policies or procedures in place in the organization relating to privacy and/or personal information.

- 17. To what extent are individuals aware of the organizations policies?**

Who is aware of such policies and procedures (e.g., business staff, clients, the general public, etc.)?