Destruction and anonymization

Destruction of documents containing personal information

As a representative of a public body or company, you are responsible for ensuring the confidential management of personal information, from its collection to its destruction, in accordance with applicable laws.

Has the purpose for which the personal information was collected been met? If so, you have an immediate obligation to destroy the personal information securely. The only restriction on this destruction requirement is the time period required by law or by a retention schedule established by government regulations (e.g., for tax obligations).

- Learn how to destroy documents containing personal information.

Destruction or possible anonymization

Effective September 22, 2023, applicable laws provide an alternative to the destruction of personal information. Once the purpose of its collection has been fulfilled, personal information may be kept by **anonymizing** it for use in the public interest (for public bodies) or for serious and legitimate purposes (for businesses):

- **Information about an individual is anonymized when it is reasonable, at any time, to anticipate under the circumstances that it no longer irreversibly identifies that person directly or indirectly.**

You must exercise care and vigilance if you intend to anonymize personal information in this context. This is a complex process aimed at ensuring that an individual cannot be re-identified by any type of technological means.

In addition, to be retained rather than destroyed, the information must be anonymized in accordance with generally accepted best practices and the **criteria and procedures determined by government regulations.** In the absence of government regulations, information cannot be anonymized to be kept or used for a public purpose or for serious and legitimate purposes.

The public body or company that collects personal information must develop and implement governance rules regarding its destruction. These rules must also refer to anonymization, if applicable.

OSLER UNOFFICIAL TRANSLATION OF CAI GUIDANCE

The Commission's view on anonymization

In light of current and future technological advances, the Commission believes that it is virtually impossible to certify that there is no possibility of anonymized information being potentially re-identified.

Some information is so distinctive in nature that it cannot be properly anonymized. An example would be genetic, biometric or geolocation information.

Anonymization of personal information implies the risk of privacy incidents. The Privacy Act also provides penalties for any person who attempts to identify an individual based on anonymized information.

Updated: May 24, 2023

Destruction procedure

Destruction of personal information: responsibility of public bodies and companies

Personal information has its own life cycle, from collection to destruction, including use and retention, and sometimes disclosure to third parties.

As a representative of a public body or company, you have an obligation to protect personal information. In terms of security and destruction, there are rules in applicable laws.

You must take proper security measures to ensure the protection of personal information that is collected, used, disclosed, retained or destroyed. These measures must be reasonable, particularly given their sensitivity, the purpose of their use, their quantity, their distribution and the medium involved.

It is important to remember that once the purposes for which personal information was collected or used have been fulfilled, the organization must destroy or **anonymize** the information.

Proper identification and management to ensure proper destruction

The Commission recommends that you first set up a document management procedure and identify persons in charge of making sure that it is properly applied.

OSLER UNOFFICIAL TRANSLATION OF CAI GUIDANCE

It is important to communicate this procedure to the entire staff.

In particular, this procedure should aim to:

- Inventory the types of documents that contain personal information (human resources file, customer database, etc.)
- Define document confidentiality levels (protected, confidential and secret) based on document sensitivity, purpose, quantity, distribution and medium

Applicable laws require you to **protect the personal information contained in all types of physical or electronic documents, in the broadest sense, whether in written, graphic, audio, visual, computerized or other form.** Note that a database, for example, is considered a document.

- Distinguish between different types of media and indicate an appropriate retention and destruction method for each (e.g. paper, digital)
- Set up a retention schedule that meets legal requirements

Choose the right destruction method

The destruction method must be adapted to the medium and level of confidentiality of the documents so as to ensure that the personal information they contain is permanently destroyed.

Several techniques are used to make sure data has been permanently destroyed:

Medium used	**Possible destruction methods**
Paper (original and all copies)	• Shredder, preferably cross-cut. If the documents are highly confidential: shredder + incineration
Digital media to be reused or recycled (e.g., flash memory cards [SD, XD, etc.], USB keys, computer hard drives)	• Formatting, overwriting, digital shredding (software that securely deletes the data and writes over the deleted file locations with random data)
Non-reusable digital media (e.g., some CDs, DVDs, flash memory cards, USB keys and hard drives that will no longer be used)	• Physical destruction (e.g., shredding, crushing, surface grinding, disintegration, perforation, incineration). Most shredders can destroy CDs and DVDs • Hard drive degausser
Machines that contain hard drives (e.g., photocopiers, fax machines, scanners, printers, etc.)	• Overwriting hard drive data or removing and destroying the actual hard when machines are replaced

OSLER UNOFFICIAL TRANSLATION OF CAI GUIDANCE

Data destruction: Do it in-house or bring in a third party?

You can destroy documents that contain personal information yourself. If your equipment does not allow you to do so securely, you may also contract an outside service provider to do it. For example, you may have to call on an outside firm to permanently destroy the data on a hard drive.

When a third party (service provider) is involved, you need a written contract that specifies certain items, including:

- The destruction process used
- That the service provider acknowledges the confidentiality of the information and agrees not to keep it for its own purposes
- That the service provider will inform its client if it uses a subcontractor for destruction
- That employees will sign a confidentiality agreement
- That the storage location containing the documents to be destroyed is secure
- That the client has access to the service provider's premises for the duration of the contract
- That the service provider is required to report regularly to the client on the destruction of the documents
- That the service provider must promptly notify the client in the event of a violation or attempted violation of information security or confidentiality obligations

Consider keeping the documents to be destroyed secure until they are picked up by the service provider responsible for destroying them

Lastly, if the service provider does not meet its obligations, you must terminate the contract and ask for the personal information to be returned.

Updated: May 16, 2023

OSLER UNOFFICIAL TRANSLATION OF CAI GUIDANCE

Source:

https://www.cai.gouv.qc.ca/organismes/destruction-et-anonymisation/

https://www.cai.gouv.qc.ca/organismes/procedure-de-destruction/

As accessed on: November 6, 2023, at 5:41 p.m.