Treasury Board of Canada Secretariat
Secrétariat du Conseil du Trésor du Canada
Canada

Guidelines for Privacy Breaches

Published: May 20, 2014

Published by Treasury Board of Canada, Secretariat
90 Elgin, Ottawa, Ontario, K1A 0R5, Canada

Catalogue Number: BT48-9/2014E-PDF
ISBN: 978-0-660-09807-4

This document is available on the Government of Canada website, Canada.ca

This document is available in alternative formats upon request.

Aussi offert en français sous le titre : Lignes directrices sur les atteintes à la vie privée

Guidelines for Privacy Breaches

Introduction

Canadians value their privacy and the protection of their personal information. They expect government institutions to respect the spirit and requirements of the *Privacy Act* (the Act). The Government of Canada is committed to protecting the privacy of individuals with respect to the personal information that is under their control and recognizes this is an essential element in maintaining public trust.

About this Guideline

The President of the Treasury Board, as "designated Minister" under the Act, is responsible for issuing directives and guidelines on the operations of that Act.

The Guidelines for Privacy Breaches provides guidance to institutions on the management of privacy breaches. These Guidelines deal with general requirements under section 4 to 8 of the Act with respect to the collection, retention, use, disclosure and disposition of personal information.

The *Policy on Privacy Protection* and the *Directive on Privacy Practices*, which support the Act, require institutions to establish plans and procedures for addressing privacy breaches. The Guidelines should also be used in conjunction with these two policy instruments in addition to the Privacy Breach Management Toolkit which was also developed to assist institutions in the privacy breach management process.

1. What is a Privacy Breach?

A privacy breach involves improper or unauthorized collection, use, disclosure, retention or disposal of personal information. These Guidelines focus primarily on improper or unauthorized access to, or disclosure of, personal information as defined in the Act.

A privacy breach may occur within an institution or off-site and may be the result of inadvertent errors or malicious actions by employees, third parties, partners in information-sharing agreements or intruders.

2. Potential causes of privacy breaches

Examples of situations that could result in the disclosure of, or access to, personal information by unauthorized parties are:

- The theft, loss or disappearance of equipment or devices containing personal information;
- The sale or disposal of equipment or devices containing personal information without purging prior to sale or disposal;
- The transfer of equipment or devices without adequate security measures;
- The use of equipment or devices to transport or store personal information outside the office for telework or off-site work arrangements without adequate security measures;
- The inappropriate use of electronic devices to transmit personal information, including telecommunication devices;
- Intrusions that result in unauthorized access to personal information held in office buildings, file storage containers, computer applications, systems, or other equipment and devices;
- Low level of privacy awareness among employees, contractors or other third parties that handle personal information;
- Inadequate security and access controls for information in print or electronic format, on site or off-site;
- The absence of provisions or inadequate provisions to protect privacy in contracts or in information-sharing agreements involving personal information;
- Insufficient measures to control access and editing rights to personal information, which may result in wrongful access to, and the possible tampering with, records containing personal information;
- Phishing or the use of deceptive tactics to trick an individual into providing their personal information either directly or by going to a fake web site. For example, an individual pretending to perform system maintenance calls a government employee to obtain his or her security password; and
- Pharming or the use of a fake copy of an official Government of Canada web site to redirect to a malicious web site in order to steal information without the users knowledge. This method takes advantage of the weaknesses in the Data Network System (DNS). For example, an individual accesses what he or she believes is an official government web site and submits personal information as requested by the site. The individual is unaware that he or she has been redirected to a fake copy of the official web site.

3. Preventing privacy breaches

To prevent a privacy breach institutions should:

- Follow the requirements of the *Policy on Government Security* (PGS) and other security direction issued by the Treasury Board of Canada Secretariat (TBS). The Royal Canadian Mounted Police (RCMP) and the Communications Security Establishment Canada (CSEC) also issue direction on physical and information technology security, respectively;
- Conduct Privacy Impact Assessments (PIAs) and Threat and Risk Assessments (TRAs) in accordance with the *Directive on Privacy Impact Assessment*;
- Take privacy into account before making contracting decisions or entering into information-sharing agreements. Government

institutions should include adequate privacy protection provisions, such as a requirement to immediately notify the government institution of a privacy breach. For more information, consult the TBS *Guidance Document: Taking Privacy into Account Before Making Contracting Decisions*;
- Provide regular and ongoing training to employees, managers and executives to ensure that they are aware of the requirements of the Code of Fair Information Practices (sections 4 to 8 of the *Privacy Act*), related TBS policies, and departmental or agency security and privacy practices and procedures;
- Ensure that personnel working off-site are aware of their privacy and security responsibilities. This means ensuring that appropriate measures are taken to safeguard the personal information they handle off-site. Government institutions should consider keeping personal information in-house when telework or similar arrangements would involve considerable privacy risks (e.g., a large volume of personal information or sensitive personal data);
- Establish clear administrative controls that restrict access and editing rights to records containing personal information to only those employees who have a legitimate need to know, and for institutions to put in place appropriate audit trails to ensure that these administrative controls are functioning as intended;
- Use cryptography (encryption) to protect sensitive personal information stored in a computer or a portable storage device or being transmitted through email, on a government network, a wireless network, or across the Internet. The *PGS* provides further direction on encryption;
- Establish clear procedures for the use of wireless devices (e.g., use of peer-to-peer [PIN-to-PIN] communications);
- As a general rule, do not send personal information by facsimile unless absolutely necessary. If you must fax personal information, consider the safeguards recommended by the Office of the Privacy Commissioner of Canada for faxing personal information;
- Purge all equipment and other electronic devices containing personal information in accordance with RCMP guidelines and CSEC guidelines before selling, disposing of, or transferring such equipment or devices;
- Empty security containers such as file cabinets, safes or mobile shelving units and ensure that no classified or protected material is left inside before selling or transferring them to other responsibility centres or outside the government;
- Take precautions against “phishing” and “pharming”:
    - Ensure that requests for personal information are valid and that individuals asking for personal information are who they claim to be;
    - Refuse to provide personal information in response to an unsolicited telephone call, fax, letter, email attachment or Internet advertisement;
    - Be on the lookout for clues indicating that a website may be fraudulent (e.g., spelling errors, unusual advertisements, or portions of the site that do not work properly);
    - Check the lock icon at the bottom of your browser to ensure that you are sending personal information over a secure connection; and
    - Verify the phone number and call the organization to determine validity if you have any concerns.
- Notify the Departmental Security Officer immediately of situations where personal data is at risk of being compromised and a potential privacy breach may occur.

4. Privacy Breach Management Process

Institutions should consult the Privacy Breach Management Toolkit for effective privacy practices, plans and procedures to address privacy breaches.

Examples of best practices in managing privacy breaches include:

- Preliminary assessment and containment;
- Full assessment;
- Notification (to affected individuals and internal management where required);
- Mitigation and prevention;
- Notification of the Office of the Privacy Commissioner of Canada (OPC) and the TBS; and
- Sharing of lessons learned.

Role of Offices of Primary Interest (OPIs)

Offices of Primary Interest (OPIs) are responsible for taking immediate action to stop the breach and to secure the affected records, systems or web sites by:

- Removing, moving or segregating exposed information or files to prevent further wrongful access;
- Shutting down the web site, application or device temporarily to permit a complete assessment of the breach and resolve vulnerabilities;
- Attempting to retrieve any documents or copies of documents that were wrongfully disclosed or taken by an unauthorized person; and
- Returning the documents to their original location or to the intended recipient unless retention is necessary for evidentiary purposes. To determine the latter, institutions should consult legal counsel.

OPIs are to also document the privacy breach by:

- Describing the circumstances that gave rise to the privacy breach. The OPI Preliminary Assessment and Containment tool and the Preliminary Assessment form can assist with the investigation of the privacy breach. Both the tool and the form can be found in the Privacy Breach Management Toolkit;
- Taking inventory of the personal information that was or may have been compromised;
- Identifying the parties whose personal information has been wrongfully disclosed or accessed, stolen or lost;

- Identifying the institutional sector or third party that is responsible for the personal information involved;
- Providing other relevant information (e.g., similar or related incidents);
- Identifying the individuals affected by the breach, or if this is not possible, identifying the groups of individuals likely to have been affected. The institution should also document the process that it carries out to identify affected individuals; and
- Notifying the departmental Access to Information and Privacy (ATIP) Coordinator or the delegated authority for privacy as well as the Departmental Security Officer (DSO). Most privacy breaches involve a breach of security. It is important to involve the ATIP Coordinator or delegated authority and the DSO to ensure that the privacy of individuals and the security of assets are taken into account in the resolution process.

Role of Departmental Security Officers

Under the *PGS*, departments must establish policies and procedures to deal with security incidents (most privacy breaches involve a breach of security). In most departments, DSOs are charged with investigating security incidents.

Depending on the process established, either the ATIP Coordinator, delegated authority or the official responsible for security should notify the Deputy Head and communications when required.

- If the breach has or could become a matter of public interest, communications officials should be notified so that communications material may be prepared to answer questions from the public, from the media, or in the House of Commons. However, personal information should be de-identified and not disclosed to Communications staff.

When a security incident results in a privacy breach, the DSO should conduct an investigation to identify deficiencies in security procedures or processes and should make recommendations where appropriate or when necessary to do so. If required under the *PGS*, the matter will be reported to law enforcement agencies. If the breach has an impact on national security, the incident should also be reported to the Canadian Security Intelligence Service.

Both the Privacy and the Security offices should establish an internal process for managing and tracking privacy breaches, which may include:

- The revision of internal procedures and policies;
- Additional training for employees;
- Restrictions on employees' access to certain personal information, based on roles and responsibilities and the need-to-know principle;
- The encryption of personal information; and
- Clearer measures in contracts to deal with breaches of privacy.

Role of ATIP Coordinators

As required by the *Directive on Privacy Practices*, institutions and their delegated authorities are required to establish plans and procedures for addressing privacy breaches. This requirement usually falls to the ATIP Coordinator.

ATIP Coordinator and their offices are responsible for investigating and managing the life cycle of a privacy breach and notifying TBS and the OPC when required. They are the single liaison for the institution when notifying the OPC and TBS.

1. Institutions should maintain a record of all privacy breaches.

- The record should include information as to the nature and extent of the breach, the type of personal information involved, the parties' involved, anticipated risks, steps taken or to be taken to notify individuals, any remedial action taken and whether the investigation determined it to be a material privacy breach.
- Records documenting privacy breaches should not contain personal information.
- Institutions should document every decision to not notify the OPC and the TBS in a standard corporate record, including the supporting rationale.
- Institutions should consider and respond to any advice and recommendations given by the OPC to mitigate risks of reoccurrence.
- Institutions can use the Privacy Breach Management Reporting Tool found in the Privacy Breach Management Toolkit to help maintain these records.

2. Institutions should consider notifying individuals whose personal information has been wrongfully disclosed, stolen or lost.

- To the extent possible, it is strongly recommended that institutions notify all affected individuals whose personal information has been or may have been compromised through theft, loss or unauthorized disclosure, especially if the breach:
    - Involves sensitive personal data such as financial or medical information, or personal identifiers such as the Social Insurance Number;
    - Can result in identity theft or some other related fraud; or
    - Can otherwise cause harm or embarrassment detrimental to the individual's career, reputation, financial position, safety, health or well-being.
- Notification should occur as soon as possible following the breach to allow individuals to take actions to protect themselves against, or mitigate the damage from, identity theft or other possible harm.
- Consult with the DSO and with law enforcement authorities to determine whether notification should be delayed to ensure that any possible investigation is not compromised.

- Care should be exercised in the notification process to not unduly alarm individuals, especially where the institution only suspects but cannot confirm that certain individuals have been affected by the breach.
- It is always preferable to notify affected individuals by letter (first class recommended), by telephone or in person, unless the individuals cannot be located or the number of individuals is so large that the task would become too onerous. Sample letters can be found in the Privacy Breach Management Toolkit.

In such cases, the institution could post a conspicuous notice on its web site or on log-in screens used to access departmental data and/or use major local or national media (television, radio, newspapers and magazines). The institution should use electronic mail only when the individual has previously consented to the receipt of electronic notices.

3. Notification of affected individuals should include:

- A general description of the incident, including date and time;
- The source of the breach (an institution, a contracted party, or a party to a sharing agreement);
- A list of the personal information that has been or may have been compromised;
- A description of the measures taken or to be taken to retrieve the personal information, contain the breach and prevent reoccurrence;
- Advice to the individual to mitigate risks of identity theft or to deal with compromised personal information (e.g., Social Insurance Number);
- The name and contact information of an official at the institution with whom individuals can discuss the matter further or obtain assistance;
- A reference to the effect that the OPC has been notified of the nature of the breach and that the individual has a right of complaint to that office, when applicable; and
- The institution should also inform affected individuals of developments as the matter is further investigated and outstanding issues are resolved.

4. Institutions and their delegates must establish a process for the mandatory reporting of material privacy breaches to the Office of the Privacy Commissioner (OPC) and the Treasury Board of Canada Secretariat (TBS). These procedures must align with the Policy on Government Security (PGS).

- A breach is deemed “material” if the breach:
    - Involves sensitive personal information; and
    - Could reasonably be expected to cause serious injury or harm to the individual and/or involves a large number of affected individuals.
- Examples of sensitive personal information could include but not limited to:
    - Medical, psychiatric or psychological information;
    - Information compiled and identifiable as part of an investigation into a possible violation of law;
    - Criminal history;
    - Information on the eligibility for social benefits or the determination of benefit levels;
    - Information describing an individual’s finances (income, liabilities, net worth, bank balances, tax returns, financial history or activities, or credit history); or
    - Information concerning an individual’s racial or ethnic origin or religious or political beliefs and associations or lifestyle.
- Examples of serious injury or harm to the individual include:
    - Identity theft or other related fraud;
    - Material loss to the individual; or
    - Lasting harm or embarrassment that will have direct negative effects on a litigation involving the individual or on an individual’s career, reputation, financial position, safety, health or well-being.

Material Privacy Breach reporting forms can be found on the OPC’s web site entitled Breach Report to the Office of the Privacy Commissioner. The same completed form must be sent to both the OPC and to the TBS. When completing the privacy breach reporting form institutions must not include any personal information.

5. Follow-Up

The institution should:

- Ensure that a plan is developed to mitigate the risks identified during the investigation and that the plan is implemented; and
- Inform the OPC and affected parties, when necessary, of any risk mitigation plan to be implemented.

6. Links to relevant policies and guidelines

Treasury Board of Canada Secretariat

- Guidance Document: Taking Privacy into account before making Contract Decisions
- Directive on Privacy Impact Assessment
- Policy on Government Security
- Operational Security Standard: Management of Information Technology Security (MITS)
- Operational Security Standard on Physical Security
- Policy on Privacy Protection

- Security Organization and Administration Standard
- Privacy Breach Management Toolkit

Royal Canadian Mounted Police

- Physical Security
- Publications, Policy Instruments and Guidelines

Communications Security Establishment Canada

- CSE Guidelines on Clearing and declassifying electronic data storage

Office of the Privacy Commissioner of Canada

- Office of the Privacy Commissioner - fact sheets
- Breach Report to the Office of the Privacy Commissioner

Questions regarding the content of these guidelines should be directed to the institution's privacy and security experts, who may in turn consult the Treasury Board of Canada Secretariat at ippd-dpiprp@tbs-sct.gc.ca