Protection of Privacy Policy

Policy Statement

The City of Hamilton recognizes that it is responsible for information assets created through the provision and management of city services. Ensuring sensitive personal information is protected is integral to maintaining public trust and confidence in government.

The City is legislatively obligated to protect personal information under *the Municipal Freedom of Information & Protection of Privacy Act* (MFIPPA) and the *Personal Health Information Protection Act* (PHIPA). The City is committed to protecting the privacy of individuals while balancing an open, transparent and accessible approach to governing.

The City will embed the protection of privacy 'into the design and architecture of IT systems and business practices'.[1]

Purpose

The purpose of this policy is to establish staff accountability, define roles and responsibilities and support staff through legislated privacy requirements and guidelines. All City Departments shall adhere to the requirements of MFIPPA in respect of exemptions to disclosure of sensitive personal and confidential information.

MFIPPA provides a formal right of access to records that are in the City's custody, or under its control, subject to limited and specific exemptions to disclosure. MFIPPA also provides individuals with an expectation of privacy.

Application

This policy applies to:

- All personal information including personal health information in the custody and control of the City, not limited by the scope of any individual statute or regulation.
- All City employees including full-time, part-time, casual, contract, volunteer and student/co-op placement employees hired or placed by the City.
- Vendors, contractors or consultants working for the City. They are required to uphold MFIPPA requirements and are subject to the same obligations for the handling of personal information, including privacy breach reporting. Departments are required to include MFIPPA obligations when contracting with Vendors and under Vendor

[1] Privacy by Design *The 7 Foundational Principles*, Ann Cavoukian, Ph.D

Performance Management obligations, this includes undertaking privacy impact assessments and identifying privacy design obligations when a Vendor is handling personal information on behalf of the City.

- The delivery of services, systems and activities that manage information within the City. Privacy obligations and overall governance of personal information must be considered within existing policies and practices of the City.

This Policy does not apply to:

- Personal information and/or constituency records of Members of Council, and/or Council appointees, which are not considered to be in the custody and control of the City. The use of personal and confidential information by elected officials and or appointee's is governed by the Code of Conduct. Complaints regarding the misuse of such information are investigated by the City's Integrity Commissioner.
- The City's Auditor General and Integrity Commissioner / Lobbyist Registrar are directly accountable to City Council. The Municipal Act requires that these officers perform their duties in an independent matter and establishes confidentiality requirements of their information.
- Separate institutions as defined under MFIPPA, including but not limited to Library Board, Police Services Board, CityHousing Hamilton.
- Information subject to legislation that overrides the privacy provisions of MFIPPA.

Policy Requirements

Personal Information - Protection of Personal Privacy

One of the key principles of the *Municipal Freedom of Information and Protection of Privacy Act* is the protection of personal privacy. For the definition of personal information, see Appendix A entitled 'What is Personal Information'.

Collection of Personal Information

The City's employees, or agents acting on the City's behalf, shall only collect personal information that they are authorized to collect. This authority can be one of the following:

- collection of the information is expressly authorized by provincial or federal legislation;
- the information is used for the purposes of law enforcement; or,
- the information is necessary to the proper administration of a lawfully authorized activity.

The City shall only collect personal information directly from the individual to whom it relates, except in circumstances set out in MFIPPA or other legislation. Examples of these include:

- where the individual authorizes another method of collection;
- the personal information may be disclosed to the City under the authority of the Freedom of Information and Protection of Privacy Act ("FIPPA");
- where the Information & Privacy Commissioner of Ontario (IPC) has authorized the City to collect the information indirectly from another person;
- the information is collected for the purpose of law enforcement; and,
- where other legislation provides for a different method of collection.

When collecting personal information, the City must provide the individual with a notice of collection statement that contains:

- the City's legal authority to collect the information;
- the principal purposes for which the information is intended to be used; and,
- the title, business address and telephone number of an officer or employee who can answer questions about the collection (why it is being collected, how it will be used).

Notice of collection statements are prepared by staff in consultation with the Privacy staff. See Appendix B attached entitled Providing Notice of Collection.

Use of Personal Information

The City is required to take reasonable steps to ensure that personal information is not used unless it is accurate and up to date. The City may only use information if the use is consistent with the purpose for which it was collected. Any other use may only occur with the expressed consent of the individual.

The City is only permitted to use personal information:

- if the individual has consented to the particular information being used;
- for the purpose for which it was obtained or compiled;
- for a consistent purpose, (i.e. the individual might reasonably expect the use);
- for a purpose permitted by MFIPPA or other legislation; or
- for the purpose for which the information was collected by the City under MFIPPA.

Disclosure of Personal Information

The City is only permitted to disclose personal information in the following circumstances:

- in compliance with Part I of the Act – Right of Access, or other provisions of MFIPPA;
- if the individual has consented to its disclosure;
- for the purpose for which it was collected;
- for a consistent purpose, (i.e. the individual might reasonably expect the disclosure);

- disclosure is made to an employee, consultant or agent of the City who needs the record in the performance of their duties, and if the disclosure is necessary and proper in the discharge of the City's functions;
- to comply with federal or provincial legislation;
- to a law enforcement agency in Canada to aid an investigation;
- in compelling circumstances affecting personal health or safety;
- in compassionate circumstances, (to contact next of kin or friend of an injured, ill or deceased person);
- to a provincial or federal government department for auditing of cost-shared programs; and
- as specifically permitted by other legislation.

Retention of Personal Information

Personal information that has been collected by the City shall be retained for at least one year after it is used, unless another retention period has been provided in the City's Records Retention by-law 11-040, as amended, or the individual has consented to its earlier disposal. The purpose of this retention period is to ensure that individuals have a reasonable opportunity to obtain access to their personal information.

Privacy Complaints and Investigations

Individuals may submit a complaint to the Information & Privacy Commissioner of Ontario (IPC) if they believe that the City of Hamilton has improperly collected, used, disclosed, retained or disposed of their personal information. The City Clerk shall receive notice from the IPC in the event that an individual has lodged a complaint and an investigation is being undertaken.

The City's corporate Privacy Office shall, in consultation with appropriate Division staff, represent the institution during a privacy complaint investigation. The responsible Divisional employee shall cooperate and assist the Privacy Office during the course of the investigation.

Responding to a Privacy Breach Under the Act

Upon learning of a privacy breach or a potential privacy breach under MFIPPA, staff shall immediately notify their Manager and the Privacy Office. The Privacy Office will assist the responsible employee in responding to the breach of personal privacy.

See Appendix C for Guidelines on Managing Privacy Breaches.

Roles and Responsibilities

Employees

- Protect privacy in executing operational duties and ensure personal information is handled with care and confidentiality in all City activities.
- Ensure the collection, use and disclosure of personal information is consistent with obligations of MFIPPA and guidance of the IPC and Privacy Office.
- Only collect personal information with proper authority and informed consent and only collect information necessary and proper in the discharge of the Division's functions.
- Ensure personal information is accessed only as required to carry out assigned duties and service delivery.
- Report a potential privacy breach to a supervisor/manager immediately if unauthorized access, collection, or dissemination of information is suspected. Assistance is sought to contain and assess impact and response to a potential breach.
- Take mandatory privacy awareness training for the appropriate handling of personal information to understand responsibilities and protect privacy in the performance of their duties.
- Take reasonable steps to ensure that personal information is not used unless it is accurate and up to date.
- Ensure privacy obligations and impact is assessed for all projects that handle data through the completion of a Privacy Impact Assessment. Project management must include an assessment of data architecture, a review of governance obligations, and required safeguards.
- Ensure Vendor contracts and performance complies with all privacy requirements, including mandatory breach response and reporting to the City.

Management within each Department

- Promote a culture and business practices that ensure City information is accessible, while respecting legislative requirements and the principles for responsible collection, use, protection and disclosure of personal information set out in this policy;
- Ensure that policies, procedures, and privacy breach reporting requirements are followed to prevent unauthorized use or disclosure of personal information. This may include security and safeguarding protocols for information management and data governance within a Department/Division, between Departments/Divisions, Vendor responsibilities, and external access.
- Ensure that the retention of personal information under the custody and control of the City is in keeping with this Policy and the Records Retention By-law 11-040;

- When introducing new services, programs, systems and technologies, prepare a Privacy Impact Assessment to address privacy implications, as required, in compliance with the principles set out in this policy;
- With respect to information security, ensure all information is protected and cannot be accessed by unauthorized individuals and processes are in place to maintain its integrity;
- Ensure privacy is embedded into the creation of all procedures for the collection, use, protection and disclosure of personal information by City employees and third parties (e.g. vendors, contractors);
- Release requested personal information directly to a requesting individual, when the information does not fall under one of the exemptions to disclosure of personal information set out in Section 38 of MFIPPA. When not permitting the release of personal information to the individual to whom it pertains, advise that individual that they may file a formal request for access to information from the Access & Privacy Office; and
- Report apparent and suspected breaches of privacy to the Privacy Office immediately, taking steps to contain the breach and mitigate privacy risks as first priority.

Medical Officer of Health

- Responsible and accountable for overseeing the administration of the Personal Health Information Protection Act (PHIPA)

City Clerk

- Responsible and accountable for overseeing the administration of the *Municipal Freedom of Information & Protection of Privacy Act* (MFIPPA), and the *Personal Information Protection and Electronic Documents Act* (PIPEDA) within the municipality and for decisions made under the above legislation;
- Ensure oversight and compliance with this policy; and
- Investigate and respond to privacy complaints received from the Information Privacy Commissioner of Ontario (IPC).

Director of Information Technology

- Ensure all information handled on behalf of a Department is subject to IT architecture and governance that upholds the data use and access restrictions required under the consent and use for which the information was collected.
- Ensure Privacy by Design principles, attached as Appendix D, privacy risk assessment and data architecture is integrated throughout IT project design, security assessment, business impact assessment, and project management governance, in cooperation with the Privacy Office.

- Ensure platforms, data handling protocols, data analytics, and associated governance do not create or access personally identifiable information without consent.
- Ensure IT Vendor obligations uphold MFIPPA requirements.
- Establish clear breach response protocols for all IT data architecture projects
- Establish audit trail best practices that are supported by technology tools in place within the City to ensure unauthorized internal access to information is monitored and reported.

Manager, Corporate Records and Freedom of Information (Office of the City Clerk, Privacy Office)

- Manage the corporate Privacy Office;
- Provide advice and establish standards, protocols and procedures to support this policy;
- Review Departmental guidelines and procedures with respect to privacy upon request from the Department;
- Review and make recommendations regarding the privacy impact of new and existing City services, programs, systems and technologies upon request from the Department (i.e. conduct Privacy Impact Assessments);
- Develop privacy awareness tools and training and make available to all City staff to improve privacy awareness; and
- Investigate reports of privacy breaches and complaints of the misuse of personal information brought to their attention by City staff and advise staff on their response.

Program Manager, Healthy and Safe Communities

- Provide advice and establish standards, protocols and procedures to support the *Personal Health Information Protection Act* (PHIPA);
- Investigate reports of privacy breaches and complaints of the misuse of personal health information brought to their attention by City staff and advise staff on their response.

Monitoring

The City Clerk shall be responsible for receiving complaints or concerns related to this policy.

Legislative and Administrative Authorities

The *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA) governs the collection, use and disclosure of information by certain institutions in Ontario including municipalities, public library boards, and police services boards. The purpose of MFIPPA is to provide a right of access to information in the custody of and under the control of the institutions with the principle that information should be made available to the public and that necessary

exemptions from the right of access should be limited and specific. The purpose of MFIPPA is also to protect the privacy of individuals with respect to personal information about themselves held by institutions and to provide individuals with a right of access to that information.

The *Personal Health Information Protection Act* (PHIPA) sets out rules for the collection, use and disclosure of personal health information. These rules will apply to all health information custodians operating within the province of Ontario and to individuals and organizations that receive personal health information from health information custodians. The rules recognize the unique character of personal health information – as one of the most sensitive types of personal information that is frequently shared for a variety of purposes, including care and treatment, health research, and managing our publicly funded health care system.

The *Personal Information Protection and Electronic Documents Act* (PIPEDA) is a Canadian law relating to data privacy. It governs how private sector organizations collect, use and disclose personal information in the course of commercial business. In addition, the Act contains various provisions to facilitate the use of electronic documents. PIPEDA became law on 13 April 2000 to promote consumer trust in electronic commerce. The act was also intended to reassure the European Union that the Canadian privacy law was adequate to protect the personal information of European citizens.

Definitions

Collection means the collection of personal information from or about the individual to whom the information relates including unintended or unprompted receipt.

Disclosure means the release of personal information by any method (e.g., sharing information by any means such as verbally, sending an email, posting online) to anybody or person.

Disposition means the action taken with regards to personal information including destruction, transfer to another entity, or permanent preservation.

Information Management means planning, creating, capturing, organizing, protecting, using, controlling, sharing, disposing of its information assets through which the value of that information is identified, and trusted.

Personal information is recorded information about an identifiable individual. Refer to section 2 (1) of MFIPPA for additional information.

http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_90m56_e.htm

Personal Health Information is identifying information about an individual that relates to their health or providing health care to the individual. Refer to section 4 PHIPA for additional information:

http://www.e- laws.gov.on.ca/html/statutes/english/elaws_statutes_04p03_e.htm#BK5

Privacy by Design means to build privacy and data protection, into the design specifications and architecture of information and communication systems and technologies at the beginning, in order to facilitate compliance with privacy and data protection principles. http://www.privacybydesign.ca/

Privacy breach means the improper or unauthorized creation, collection, use, disclosure, retention or disposition of personal information.

Privacy Impact Assessment (PIA) is a process for identifying, assessing and mitigating privacy risks.

Use means the purpose(s) for which the information was obtained or compiled.

Confidential information means information that is subject to the exemptions to disclosure found in s. 9 (Relations with Governments), s. 10 (Third Party Proprietary Information) and s. 14 (1) (Personal Privacy) of MFIPPA, as well as any other information that the City deems to be confidential.

References

Privacy by Design Principles – Information & Privacy Commissioner of Ontario
Municipal Freedom of Information & Protection of Privacy Act
Records Retention By-law 11-040, as amended

Appendices

Appendix A – What is Personal Information
Appendix B – Providing Notice of Collection
Appendix C – Guidelines on Managing Privacy Breaches
Appendix D – Privacy by Design Principles

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

Fact Sheet

What is Personal Information?

October 2016

INTRODUCTION

The *Freedom of Information and Protection of Privacy Act (FIPPA)* and the *Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)* (the acts) protect the privacy of personal information while providing individuals with a right of access to their own information.

In this fact sheet, we provide guidance about how the Information and Privacy Commissioner (IPC) interprets the term "personal information."

HOW IS PERSONAL INFORMATION DEFINED IN THE ACTS?

The acts define personal information as "recorded information about an identifiable individual," and include a list of examples of personal information (see Appendix A for the full definition).

Recorded information

Information can be recorded in any format, such as paper records, electronic records, digital photographs, videos or maps.

About an identifiable individual

Information is about an identifiable individual if:

- it is about the individual in a personal capacity; that is, it reveals something of a personal nature about the individual, and
- it is reasonable to expect that an individual can be identified from the information (either alone or by combining it with other information)

The listed examples include a person's name when combined with other information about them, such as their address, sex, age, education, or medical history. These examples are not exhaustive and many other kinds of information may still qualify as personal information.

FREQUENTLY ASKED QUESTIONS

What if an individual is acting in a business, professional or official capacity?

The acts specifically exclude from the definition of personal information the name, title, contact information or designation that identifies a person in a business, professional or official capacity. This includes a business carried out in a home.

As a general rule, information about an individual in a business, professional or official capacity is not considered to be personal information.

However, even if information relates to an individual in such a capacity, it may still qualify as personal information if it reveals something of a personal nature about the individual. The context in which the information appears is important.

Is an address personal information?

An address, by itself, is not personal information because it is about a property and not an individual. However, information about a property can qualify as personal information if it reveals something personal. For example, a police service placed a lawn sign on a property stating that it was the site of a search warrant for illicit drugs. The IPC decided that the address on the sign was personal information because it revealed allegations of criminal activity against individuals associated with the property.

Does an individual's name qualify as personal information?

Like an address, a name by itself is not personal information. A name is personal information if it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual.

Can information about a business be personal information?

Generally, business information is not considered personal information. The term "individual" in the definition of personal information means that it only relates to natural persons. Sometimes confidential business information is confused with personal information. Business information may hold tremendous value and importance for organizations, but it is not personal information.

Is information about deceased individuals their personal information?

Information about an individual is not personal information if they have been dead for more than thirty years.

CONCLUSION

It is important to examine the context in which information appears in determining whether the information is "about" an individual and whether the individual is "identifiable." Depending on the context, information may not meet the definition of personal information because it is, for example, information about a property or business, or about an individual in a business capacity. You can find IPC orders and complaint reports regarding the definition of personal information on the IPC's website (**www.ipc.on.ca**).

APPENDIX

Definition of "personal information" in the acts

"personal information" means recorded information about an identifiable individual, including,

(a) information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual,

(b) information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,

(c) any identifying number, symbol or other particular assigned to the individual,

(d) the address, telephone number, fingerprints or blood type of the individual,

(e) the personal opinions or views of the individual except where they relate to another individual,

(f) correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence,

(g) the views or opinions of another individual about the individual, and

(h) the individual's name where it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual.

IPC

Practices

NUMBERS

REVISED SEPTEMBER 1998

PUTTING ONTARIO'S INFORMATION AND PRIVACY LEGISLATION TO WORK

INFORMATION AND PRIVACY COMMISSIONER/ONTARIO

ANN CAVOUKIAN, Ph.D., COMMISSIONER

Providing Notice of Collection

Under the Freedom of Information and Protection of Privacy Act *and the* Municipal Freedom of Information and Protection of Privacy Act *(the* Acts), *government organizations must provide notice to individuals when collecting personal information - whether collection is made directly or indirectly.*

Quite often complaints received by the Information and Privacy Commissioner (/PC) are the result of the lack of notice or incomplete notice. The /PC has found that while most institutions provide notice, some are not providing adequate notice.

This issue of IPC Practices *explains the notice requirements and suggests procedures for providing proper notice.*

Section 39(2) of the provincial *Act* and section 29(2) of the municipal *Act* state that when collecting personal information, unless an exception applies, an institution **must** provide the individual to whom the personal information relates with notice which includes specific details on the following three requirements:

- the legal authority for the collection;
- the principle purpose(s) for which the personal information is intended to be used;
- the title, business address and telephone number of a person employed by the institution who can answer questions about the collection.

Manner of Providing Notice

Notice may be provided either orally - in person, over the telephone; or in writing - on an application form, on a posted sign, in a newspaper ad; or in any other mannerwhich informs the individual about the collection.

Exceptions to Providing Notice

• *provincial and municipal* Acts

Sections 39(2) and (3) of the provincial *Act* and section 29(3) of the municipalAct state that the notice requirement does not apply where:

- the Minister (who is the Chair, Management Board of Cabinet) waives notice; or
- the head cites a law enforcement exemption.

• *municipal* Act *only*

In addition, section 29(3)(c) of the municipal *Act* provides that the notice requirement does not apply if the *Act's* regulations provide that notice is not required.

Section 4 of Regulation 823 under the municipalAct states that where a head makes available to the public a statement describing the purpose(s) of the collection of personal information and the reason that notice has not been given, then the institution is not required to give notice of the collection to each individual. However, this only applies where:

- providing notice would frustrate the purpose of the collection;
- providing notice might result in an unjustifiable invasion of another individual's privacy; or
- the collection is for the purpose of determining suitability or eligibility for an award or honour.

Unsolicited Personal Information

Sometimes institutions receive personal information, such as resumes, which they did not request. If an institution does not retain unsolicited personal information, notice is not required. However, if an institution subsequently uses this personal information, for example, by placing unsolicited resumes in an inventory or by considering them at a later date, then the institution is obliged to notify the individual.

Recommended Procedures

The IPC encourages institutions to consider the following procedures for providing notice:

1. Advise all staff that under sections 38(2) of the provincial *Act* and 28(2) of the municipal *Act,* an institution must be certain that it has the authority to collect personal information, either directly or indirectly.

2. When notice is provided, ensure that the notice meets the three requirements listed in section 39(2) of the provincial Act and section 29(2) of the municipal *Act:*

   · *The legal authority for the collection:* Cite the proper legal authority that permits the collection by referring to the specific act and section which authorizes the collection. Where an act does not specifically refer to collection, provide the specific section of an act or by-law which authorizes the activity or program for which the information must be collected.

   Note: It is insufficient to say, "This information is being collected in accordance with *the Freedom of Information and Protection of Privacy Act* or the *Municipal Freedom of Information and Protection of Privacy Act.* "

   · *The principal purpose(s) for which the personal information is intended to be used:* Be sure to fully inform the individual from whom the information is collected about how the information will be used.

   Many complaints received by the !PC's Compliance department about collection, use and disclosure are the result of inadequate notice to the individual regarding the intended use of his or her personal information.

   · *The title, business address and telephone number of a person employed by the institution who can answer any questions about the collection:* Ensure that the individual will have no difficulty in contacting someone who can provide answers to questions or additional information about the collection.

3. Include procedures in your operations/procedures manual for staff to follow when giving oral or written notice. This will ensure that all staff are aware of their responsibilities to provide notice and that the notice meets the *Acts* 'three requirements.

Example of Written Notice

Here is an example of notice that may be used on a job application form:

Personal information on this form is collected under the authority of *the Municipal Act,* R.S.O. 1980, c.302 (as amended), and will be used to determine the qualifications for employment with the Town of Cityville. Questions about this collection should be directed to the Human Resources Co-ordinator, 110 Elm Street, Cityville, Ontario, L3P 2N1, (313) 234-5678.

IPC
Practices

is published regularly by the **Office of the Information and Privacy Commissioner.**

If you have any comments regarding this publication, wish to advise of a change of address or be added to the mailing list, contact:

Communications Department
Information and Privacy Commissioner/Ontario
80 Bloor Street West, Suite 1700
Toronto, Ontario M5S 2V1
Telephone: (416) 326-3333 • 1-800-387-0073
Facsimile: (416) 325-9195
TTY (Teletypewriter): (416) 325-7539
Website: http://www.ipc.on.ca

50% recycled including 20% post-consumer fibre

PRIVACY

Privacy Breaches

Guidelines for Public Sector Organizations

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

Ontario's privacy laws set out the rules for how public sector organizations should manage information about identifiable individuals – namely, personal information.

This guide explains what a privacy breach is and how to respond to one. It can also help you develop your own privacy breach response plan.

If you are an organization subject to Ontario's health privacy law, you should refer to our guidance, *Responding to a Health Privacy Breach: Guidelines for the Health Sector*.

WHAT IS A PRIVACY BREACH?

A privacy breach occurs when personal information is collected, retained, used, disclosed, or disposed of in ways that do not comply with Ontario's privacy laws. The most common privacy breaches occur when unauthorized persons gain access to personal information. For example, personal information may be seized in a cyberattack, stolen (such as through theft of a portable device) or accessed by an employee for improper purposes.

RESPONDING TO A PRIVACY BREACH

When a privacy breach occurs, you should do the following:

IMMEDIATELY ALERT APPROPRIATE PARTIES

Alert all relevant staff of the breach, including your freedom of information and privacy coordinator, and determine who else within your organization should be involved in addressing the breach.

CONTAIN THE BREACH

Identify the nature and scope of the breach and the action you need to take to contain it:

- determine what personal information is involved
- take corrective action, for example:
  - ensure that no personal information has been retained by an unauthorized recipient and get their contact information in case follow-up is required
  - ensure that the breach does not allow unauthorized access to any other personal information by taking appropriate action (for example, changing passwords or identification numbers, or temporarily shutting down a system)
  - in a case of unauthorized access by staff, consider suspending their access rights
  - retrieve hard copies of any personal information that has been disclosed

NOTIFY THOSE AFFECTED BY THE BREACH

You should notify those affected as soon as reasonably possible if you determine that the breach poses a real risk of significant harm to the individual, taking into consideration the sensitivity of the information and whether it is likely to be misused. If law enforcement is involved, ensure that notification will not interfere with any investigations.

Notification should be direct, such as by telephone, letter, email or in person. Indirect notification can be used in situations where direct notification is not possible or reasonably practical, for instance, when contact information is unknown or the breach affects a large number of people.

Notification to affected individuals should include:

- details of the extent of the breach and the specifics of the personal information that was compromised
- the steps taken and planned to address the breach, both immediate and long-term

- a suggestion, if financial information or information from government-issued documents is involved, to:
    - contact their bank, credit card company, and appropriate government departments to advise them of the breach
    - monitor and verify all bank account, credit card and other financial transaction statements for any suspicious activity
    - obtain a copy of their credit report from a credit reporting bureau
- contact information for someone within your organization who can provide additional information and assistance, and answer questions
- a statement that they have a right to make a complaint to the IPC and how to do so

INVESTIGATE

- Identify and analyze the events that led to the breach
- Review your policies and practices in protecting personal information, privacy breach response plans and staff training to determine whether changes are needed
- Determine whether the breach was a result of a systemic issue and if so, review your program-wide or institution-wide procedures
- Take corrective action to prevent similar breaches in the future and ensure your staff are adequately trained
- If you have contacted the IPC, advise us of your findings and remedial measures, and cooperate with any further investigation we undertake into the incident

NOTIFYING THE IPC

You should notify the IPC of significant breaches, such as those that may involve sensitive personal information or large numbers of individuals, or when you are having difficulties containing the breach. In these situations, you should notify the IPC as soon as reasonably possible.

In situations where you will be notifying a large number of individuals, it is important to contact the IPC before you begin the notification process, so that we are prepared to respond to inquiries.

The IPC can assist you with your breach response plan.

WHAT HAPPENS WHEN THE IPC INVESTIGATES?

When responding to a report or complaint of a privacy breach, or initiating our own investigation, we may:

- assess whether the breach has been contained and affected individuals adequately notified
- interview individuals involved
- review and provide advice on your organization's policies and any other relevant documents
- issue a report after the investigation, which may include recommendations
- issue an order

The purpose of the IPC investigation is future-oriented — that is, if there was a privacy breach, the IPC will assist the institution in taking steps to prevent similar occurrences.

HOW TO REDUCE THE RISK OF FUTURE PRIVACY BREACHES

You should consider the following measures to prevent privacy breaches:

- educate your staff about Ontario's privacy laws and your organization's policies and practices governing the collection, retention, use, security, disclosure and disposal of personal information
- conduct privacy impact assessments before introducing or changing technologies, information systems, and processes to ensure privacy risks are identified and addressed
- seek input from appropriate parties such as your legal counsel and security units, your freedom of information and privacy coordinator, the Ontario ministry responsible for information and privacy matters, and our office, as necessary

ADDITIONAL RESOURCES

The IPC has guidance that can assist your organization in meeting its privacy responsibilities and avoiding a privacy breach. You can find these documents in the guidance section of the IPC's website (**www.ipc.on.ca**).

About the IPC

The role of the Information and Privacy Commissioner is set out in the *Freedom of Information and Protection of Privacy Act*, the *Municipal Freedom of Information and Protection of Privacy Act*, and the *Personal Health In-formation Protection Act*. The commissioner is appointed by the Legislative Assembly of Ontario and is independent of the government of the day.

Information and Privacy
Commissioner of Ontario

Commissaire à l'information et à la
protection de la vie privée de l'Ontario

2 Bloor Street East, Suite 1400
Toronto, Ontario, Canada M4W 1A8
Phone: (416) 326-3333 / 1-800-387-0073
TDD/TTY: 416-325-7539

www.ipc.on.ca
info@ipc.on.ca

September 2019

Privacy by Design

The 7 Foundational Principles

Ann Cavoukian, Ph.D.
Information & Privacy Commissioner
Ontario, Canada

Privacy by Design is a concept I developed back in the 90's, to address the ever-growing and systemic effects of Information and Communication Technologies, and of large-scale networked data systems.

Privacy by Design advances the view that the future of privacy cannot be assured solely by compliance with regulatory frameworks; rather, privacy assurance must ideally become an organization's default mode of operation.

Initially, deploying Privacy-Enhancing Technologies (PETs) was seen as the solution. Today, we realize that a more substantial approach is required — extending the use of PETs to PETS *Plus* — taking a positive-sum (full functionality) approach, not zero-sum. That's the "*Plus*" in PETS *Plus*: positive-sum, not the either/or of zero-sum (a false dichotomy).

Privacy by Design extends to a "Trilogy" of encompassing applications: 1) IT systems; 2) accountable business practices; and 3) physical design and networked infrastructure.

Principles of *Privacy by Design* may be applied to all types of personal information, but should be applied with special vigour to sensitive data such as medical information and financial data. The strength of privacy measures tends to be commensurate with the sensitivity of the data.

The objectives of *Privacy by Design* — ensuring privacy and gaining personal control over one's information and, for organizations, gaining a sustainable competitive advantage — may be accomplished by practicing the following 7 Foundational Principles *(see over page)*:

The 7 Foundational Principles

1. ***Proactive*** not Reactive; ***Preventative*** not Remedial

The *Privacy by Design* (PbD) approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events *before* they happen. PbD does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred — it aims to *prevent* them from occurring. In short, *Privacy by Design* comes before-the-fact, not after.

2. Privacy as the ***Default Setting***

We can all be certain of one thing — the default rules! *Privacy by Design* seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy — it is built into the system, *by default*.

3. Privacy ***Embedded*** into Design

Privacy by Design is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.

4. Full Functionality — ***Positive-Sum***, not Zero-Sum

Privacy by Design seeks to accommodate all legitimate interests and objectives in a positive-sum "win-win" manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. *Privacy by Design* avoids the pretense of false dichotomies, such as privacy ***vs.*** security, demonstrating that it ***is*** possible to have both.

5. End-to-End Security — ***Full Lifecycle Protection***

Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved — strong security measures are essential to privacy, from start to finish. This ensures that all data are securely retained, and then securely destroyed at the end of the process, in a timely fashion. Thus, *Privacy by Design* ensures cradle to grave, secure lifecycle management of information, end-to-end.

6. ***Visibility*** and ***Transparency —*** Keep it ***Open***

Privacy by Design seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to users and providers alike. Remember, trust but verify.

7. ***Respect*** for User Privacy — Keep it ***User-Centric***

Above all, *Privacy by Design* requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric.

Revised: January 2011
Originally Published: August 2009

Information and Privacy Commissioner of Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario • CANADA • M4W 1A8
Telephone: 416-326-3333 • 1-800-387-0073
Web: www.ipc.on.ca • www.privacybydesign.ca
E-mail: info@ipc.on.ca