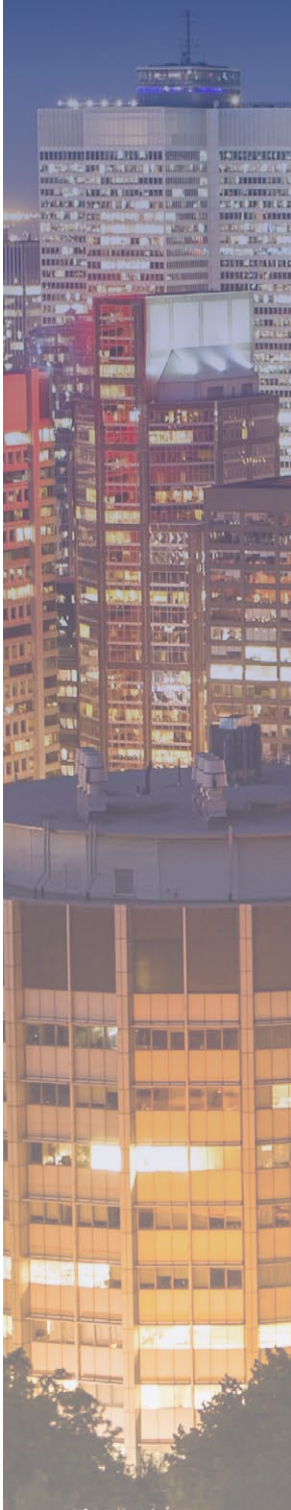
Vérificateur général
de la Ville de Montréal

# Report of the Auditor General of the Ville de Montréal
to the City Council and to the Urban Agglomeration Council

For the Year Ended December 31, 2012

5.13

# Protection of Personal Information



# Table of Contents

# List of Acronyms

| | |
|---|---|
| CAI | Commission d'accès à l'information |
| PI | personal information |
| SIN | social insurance number |
| STI | Service des technologies de l'information |

# 5.13. Protection of Personal Information

## 1. Introduction

With more than 1.6 million residents and 28,000 employees, Ville de Montréal (the city) collects and processes a considerable amount of information concerning the private life of its citizens, elected officials and employees. This information is necessary in order for the city to adequately serve the public. These activities may include, for example, processing requests from citizens (through the 311 service or borough offices) and managing employees.

In Canada, privacy is a fundamental right that is protected in a comprehensive manner by federal and provincial laws.

Adopted on June 27, 1975, Québec's Charter of Human Rights and Freedoms makes the right to privacy an intrinsic right. The charter states, among others, the following intrinsic rights and freedoms of citizens:

- the right to the safeguard of dignity, honour and reputation;
- the right to respect of private life;
- the right to respect of professional secrecy.

A true North American pioneer in the area of access to information and protection of privacy, Québec has built, over the past three decades, a legislative model that has paved the way for the implementation of similar measures throughout Canada.

Personified by Québec's Commission d'accès à l'information (CAI), this unique model is an essential reference source for all western countries in the area of access to information and protection of private life.

The CAI applies two acts:

- For the public sector: the *Act respecting access to documents held by public bodies and the protection of personal information*[1]; and
- For the private sector: the *Act respecting the protection of personal information in the private sector*[2].

1 RSQ, chapter A-2.1.
2 RSQ, chapter P-39.1.

As a municipality, the city is subject to the *Act respecting access to documents held by public bodies and the protection of personal information*. This Act sets out two intrinsic rights: the right of access and the right of protection of personal information (PI). The Act applies to all documents whether they are recorded in writing or print, on sound tape or film, in computerized form, or otherwise.

PI is defined as information that:

- identifies a natural person (as opposed to a corporate body);
- helps identify an individual (as opposed to depersonalized information);
- is factual or subjective about a person regardless of its form or support, whether recorded or not.

Given its nature, PI is confidential. The theft or disclosure of PI is often used for fraudulent purposes that can go as far as identity theft and an attack on an individual's reputation. The most sensitive types of PI are, among others, a person's:

- social insurance number (SIN);
- health insurance number;
- date of birth;
- salary and income tax statements;
- banking information;
- medical records;
- résumé.

As with any other information of a sensitive nature, the city must ensure the confidentiality of PI. To do so, it must put in place security measures to protect PI from theft, disclosure and unauthorized use.

## 2. Audit Scope

The objective of our audit was to evaluate the effectiveness of the controls put in place to ensure adequate software and physical security of the PI of citizens and employees held by the city, with the exception of information related to the Service de police de la Ville de Montréal.

To this end, we investigated the following aspects:

- **PI management frameworks:** Does the city have frameworks that define the requirements of sound PI management and that are applied to all business units?

- **PI inventory:** Is there a complete and updated PI inventory that enables the city to draw an overall picture of the PI to be protected in order to ensure its confidentiality?
- **Employee education:** Are employees aware of the issues and risks related to PI so that they are more able to comply with the security rules regarding the protection of PI?
- **Incident management:** If a major event were to occur that could result in the mass disclosure of PI, is there an incident management procedure in place that would enable the city to react in a timely manner to limit real and potential repercussions and to take the necessary measures to resolve the incident?
- **Logical access:** Are security parameters (e.g., passwords and rights of access) configured so that only authorized individuals whose work requires them to use PI can access the information systems in which PI is processed?
- **Physical access:** Are there containment mechanisms, such as a secured vault or locked filing cabinets, to restrict access to authorized persons only to PI that is on physical supports (e.g., medical records and employee records)?
- **PI retention:** Is the PI housed solely on the production environments of information systems that are used daily by employees and managers? Instead of real PI, is depersonalized PI used in test, development and training environments to limit the risks of a breach of confidentiality?
- **PI transmission:** Is PI that is sent to third parties (e.g., the CSST, the Ministère du Revenu) protected by security measures to safeguard the confidentiality of the information that is transferred?
- **PI destruction:** Is PI depersonalized or destroyed in such a way that it cannot be reconstituted to prevent any fraudulent use?

We audited the following files since they held important and sensitive PI:

- about citizens:
  - application files,
  - requests for services and complaints,
  - registration in recreational activities,
  - requests for renovation subsidies;
- about employees, elected officials, judges, commissioners and retirees:
  - employee records,
  - medical records,
  - pay records,
  - pension plan records.

At the same time, we selected the following administrative units for our audit of their PI management responsibilities and the volume of information they held and processed:

- the Direction du greffe;

- the Service du capital humain et des communications;
- the Service des technologies de l'information (STI);
- the Direction des services regroupés aux arrondissements, which reports to the Service de la concertation des arrondissements et des ressources matérielles;
- the Division de la paie institutionnelle, which reports to the Direction de la comptabilité et du contrôle financier of the Service des finances;
- the Division de la gestion des rentes, which reports to the Direction de la gestion financière of the Service des finances;
- the Division de la gestion des programmes de logement, which reports to the Direction de l'habitation of the Service de la mise en valeur du territoire;
- the Division des ressources humaines:
  - of the Service de sécurité incendie de Montréal,
  - of Saint-Laurent borough,
  - of Montréal-Nord borough,
  - of Côte-des-Neiges–Notre-Dame-de-Grâce borough,
  - of Villeray–Saint-Michel–Parc-Extension borough.

Following is the list of information systems that process the PI covered during our audit:

- SIMON RH (application files, basic employee records);
- SIMON PAIE (the pay of judges, elected officials, commissioners and retirees);
- Employeur D (medical records);
- Pay (IBM);
- GDC (the management of citizens' requests);
- Super H (employee records);
- InfoRH (data warehouse of the Service du capital humain et des communications);
- Registre des postes (employee positions and salaries);
- ARIEL (pension plans);
- Ludik (recreational activities);
- SDSR (requests for renovation subsidies).

It should be noted that our audit may, in no way, be construed as a mandate to attest to the level of compliance of the city with the *Act respecting access to documents held by public bodies and the protection of personal information.*

## 3. Findings and Recommendations

Overall, our audit did not reveal any major deficiencies in the control mechanisms put in place for the protection of PI held and processed by the city.

Table 1 presents the overall results of our audit based on the identified areas of risk.

**Table 1 – Overall Results According to the Areas of Risks**

| Areas of risks | Inherent risk[a] | Residual risk[b] |
|---|---|---|
| **PI management frameworks**<br>Disclosure of PI due to the absence of frameworks that define specific responsibilities and requirements related to protection of PI. | High[c] | Low |
| **PI inventory**<br>Breach of confidentiality of certain PI that was improperly determined during the PI inventory procedures and that was not adequately protected. | Moderate | Low |
| **Employee education**<br>Disclosure of certain PI due to the lack of knowledge on the part of employees about the behaviour to adopt to safeguard and maintain the confidentiality of PI. | High | Low |
| **Incident management**<br>Inability to address and resolve major problems in a timely manner, for example the mass disclosure of PI. | High | Low |
| **Logical access**<br>Breach of confidentiality of PI in the wake of unauthorized access to information systems. | Critical | Moderate |
| **Physical access**<br>Breach of confidentiality of certain PI in the wake of inadequate security measures applied to physical documents and files containing PI. | Critical | Low |
| **PI retention**<br>Real PI is used for environments other than those of production and could be stolen or divulged. | Critical | High |
| **PI transmission**<br>Breach of confidentiality of PI after interception during transmission between information systems. | High | Low |
| **PI destruction**<br>Reconstitution and disclosure of PI that was not destroyed in a secure and irreversible way. | Critical | Low |

[a] Gross risk, i.e. without taking into account control mechanisms.
[b] Exposure to risk after an evaluation of the control mechanisms in place.
[c] Refer to Table 2

Section 3.1 and the following sections detail the specific deficiencies found during our audit that require corrective action. We evaluated these deficiencies based on the impact levels presented in Table 2.

**Table 2 – Definitions of Impact Levels**

| Impact levels | Definition of impact levels |
|---|---|
| **Critical** | Direct consequence on individual security, major impact on the reputation of individuals and the reputation of the city if the PI were divulged |
| **High** | While there is no consequence on individual security due to the large volume of PI present, the breach of confidentiality of this information would cause major harm to the city's operations and reputation. The individuals could become victims of theft or identity theft. |
| **Moderate** | Due to the presence of certain PI, a breach of confidentiality of this information could cause moderate harm to the reputation and operations of the city. |
| **Low** | Repercussions would be negligible on the city's operations and services. Loss of trust in the city by citizens is unlikely |

## 3.1. Personal Information Present in Information System Environments Other than Production

### 3.1.A. Background and Findings

Information systems generally have several distinct environments. There is the production environment, which is used by employees in the course of their work and which contains real data that is required to meet business needs. Then there are the environments that are used for other purposes, for example:

- development environments: these are used by information technology specialists to develop or improve the functionalities of applications;
- test environments: these are used by groups of users and computer analysts to ensure that changes made to the applications function properly;
- training environments: these enable employees to acquire the expertise needed to effectively use the information systems.

In environments other than production, the use of real data is not necessary, especially if that data is confidential, as is the case with PI. There are no business needs to justify its use. Good industry practices recommend that dummy records be used in environments others than production.

During our audit, we concluded that real PI was being copied, in whole or in part, from production environments to various test and development environments. As well, no systematic PI deletion procedure was being applied once the test or development work was completed. The information systems involved are listed below.

- **SIMON (SIMON RH and SIMON PAIE):** SIMON is the city's ERP (enterprise resource planning) system. SIMON RH contains basic employee records, as well as application files. SIMON PAIE contains 14,500 pay records of elected officials, judges, commissioners and retirees. On average, a dozen environments are used for development and test purposes. Only two of these environments have a depersonalized SIN and date of birth to avoid associating them with real natural persons. The other environments contain copies, sometimes in full, of PI originating from the production environment, the most sensitive of which are, among others, the SIN, date of birth, earnings and banking information.
- **Super H:** This application contains all the employee records, as well as those of applicants, elected officials, judges, commissioners and retirees. The test environment uses real PI originating from the product environment, such as the SIN, date of birth, salary, address and home telephone number.
- **InfoRH:** This data storehouse of the Service du capital humain et des communications contains PI for all employees, as well as applicants, elected officials, judges, commissioners and retirees. The development environment contains real PI, including the SIN, date of birth, salary, address and home telephone number.
- **Registre des postes:** This application contains job information about city employees. Real PI is copied from the production environment to the test environment. Salaries, among other information, are found here.
- **Employeur D:** This system contains the medical records of employees, elected officials, judges and commissioners when medical problems arise. The test environment uses real PI originating from the production environment. This information includes, among other things, medical information, the SIN, health insurance number, date of birth and salary.
- **Paie (IBM):** This application manages the pay of most of the city's employees and contains PI related to salaries. The development and test environments contain extracts of real PI originating from the production environment. The types of PI are, among others, banking information, the SIN, earnings, home address, date of birth and income tax statements.

We estimate that the impact level is **high** since the city is facing the following potential risks: in allowing the use of real PI outside of production environments, the PI of all employees, elected officials, judges, commissioners, retirees and applicants could be stolen and disclosed to unauthorized individuals. With such information, malicious individuals could commit fraudulent acts, such as theft and identity theft. In all cases, this would seriously harm the city's reputation.

### 3.1.B. Recommendation

**We recommend that the Service du capital humain et des communications, as well as the Division de la paie institutionnelle of the Service des finances, in collaboration with the Service des technologies de l'information, put in place procedures to black out real personal information (e.g., social insurance number, date of birth) from the data of environments other than production in the information systems that they own:**

- **the Service du capital humain et des communications:**
  - **SIMON RH,**
  - **Super H,**
  - **InfoRH,**
  - **Registre des postes,**
  - **Employeur D ;**
- **the Division de la paie institutionnelle:**
  - **Paie (IBM),**
  - **SIMON PAIE.**

**Business units' responses:**

***SERVICE DU CAPITAL HUMAIN ET DES COMMUNICATIONS***

*[TRANSLATION] SIMON RH and InfoRH: We contacted the STI to have confidential data scrambled in all the environments other than production.* ***(Completed, April 2013)***

*Super H and Registre des postes: The STI has taken the necessary measures to scramble data in the "test" environment. Nevertheless, we are currently in contact with them to ensure that the information elements have been taken into consideration.* ***(Completed, April 2013)***

*Employeur D: The request has already been made to the STI to scramble confidential data.*

*Moreover, given that this application contains data related to accidents and illnesses, we are in the process of reviewing the information that will be considered confidential.* ***(Completed, March 2013)***

***SERVICE DES FINANCES***

*[TRANSLATION] A work order has been issued to STI to implement PI block-out procedures for the pay management systems.* ***(Planned completion: December 2013)***

## 3.2. Security Parameters of Non-Configured Passwords

### 3.2.A. Background and Findings

Passwords are the first line of defence in preventing unauthorized access to information systems containing sensitive and confidential data, such as PI.

Password security parameters make it possible to require users to choose robust passwords. These parameters define, among, other things, the length of the password, its complexity, its expiry deadline, and the history of recent passwords

According to the STI procedure entitled [TRANSLATION] “Standard respecting access keys to computer resources”, password requirements include:

- an expiry deadline: 90 days;
- a password length: minimum of eight characters;
- a history: six recent passwords;
- activation of password complexity (e.g., combination of alphanumeric characters, special characters, upper and lower case letters)

During our audit, we concluded that the password safety parameters had not been activated for the Employeur D application. As for Ludik, there is no safety parameter that can be activated. The only limitation on these applications is that the user must choose a password that contains at least one character. There is no expiry deadline or history of passwords. In the case of Employeur D, the password that is assigned to the user at the time access is created corresponds to his or her name, and the system does not require that it be changed when the user first logs on to the system.

We estimate the impact level to be **high** since the city faces the following potential risks: because there is no security requirement for passwords, malicious individuals could easily uncover them. Consequently, in the case of Employeur D, these individuals would have access to the sensitive PI of employees, elected officials, judges and commissioners who have had health problems (e.g., the SIN, health insurance number, date of birth, salary, medical record) and, in the case of Ludik, to 800,000 files on citizens, 15,200 of which contain SIN and health insurance numbers. If such information were divulged, these individuals could commit identify theft and not only harm the city’s reputation but also that of its employees, elected officials, judges and commissioners.

### 3.2.B. Recommendation

**We recommend that the Service du capital humain et des communications, which owns Employeur D and Ludik, in collaboration with the Service des technologies de l'information:**

- **configure the security parameters of passwords with, at the very minimum, the following requirements:**
  - **a minimum length: eight characters,**
  - **an expiry deadline: 90 days,**
  - **a history: six last passwords,**
  - **activation of password complexity;**
- **change all the current passwords as soon as possible, without waiting for the 90-day expiry deadline, to comply with the new parameters;**
- **require that new users change their initial password at the time they first log on to the system.**

**Business unit's response:**

*[TRANSLATION] In the case of the Employeur D application, measures were taken following the audit by the Bureau du vérificateur général in last December.*

*The minimum length is now eight characters with at least two numbers.*

*The expiry deadline has been configured to 90 days.*

*An announcement was sent to all users informing them of these changes.*

*All passwords have been changed.* ***(Completed, December 2012)***

*In the case of the Ludik software package, the STI is in discussions with the supplier to determine the best method to use in order to apply the recommendations and to limit the application developments of the software package.* ***(Completed, April 2013 [corrective strategy]; planned completion: to come [implementation of the strategy])***

## 3.3. Discrepancy in the Review Process of Users and their Access Rights

### 3.3.A. Background and Findings

To ensure adequate protection of PI, managing users' access rights must not only provide requirements and security mechanisms for the creation, deletion and modification of access but also include a review process of users' accounts.

A recurring review process ensures that all employees who have left the employ of the city or who have changed jobs do not keep their former access privileges.

During our audit, we concluded that there was no formal review process of users' access rights to the following information systems:

- GDC;
- Employeur D;
- SIMON RH;
- Ludik.

In the case of the Registre des postes, Super H and InfoRH information systems, a review of users' access rights is conducted yearly. In our opinion, given the critical nature of the PI, this frequency of review is insufficient.

We estimate the impact level to be **moderate** since the city faces the following potential risks: individuals who have left their job with the city could keep access rights to information systems and those who have changed jobs could keep former access rights that no longer correspond to their new duties and responsibilities. This could lead to a breach of the confidentiality of the PI held by the city.

### 3.3.B. Recommendation

**We recommend that the Direction des services regroupés aux arrondissements of the Service de la concertation des arrondissements et des resources matérielles and the Service du capital humain et des communications put in place a recurring review process (at least quarterly) of users' access rights to the information systems that they own:**

- **the Direction des services regroupés aux arrondissements:**
  - **GDC;**
- **the Service du capital humain et des communications:**
  - **Employeur D,**
  - **SIMON RH,**
  - **Super H,**
  - **Registre des postes,**
  - **InfoRH,**
  - **Ludik.**

**Business units' responses:**

***SERVICE DE LA CONCERTATION DES ARRONDISSEMENTS ET DES RESSOURCES MATÉRIELLES***

*[TRANSLATION] A quarterly report will be extracted by the GDC system driver (Section de l'expertise et du soutien 311) and sent to expert users in the 19 boroughs for access follow-up.*

*Everything will be documented and posted in an internal process at the Section de l'expertise et du soutien 311.* ***(Planned completion: May 2013)***

***SERVICE DU CAPITAL HUMAIN ET DES COMMUNICATIONS***

*[TRANSLATION] A procedure will be put in place between now and the end of April 2013 to validate access once every quarter.* ***(Completed, April 2013)***

*In the case of the Ludik software package, a procedure is in the process of being drafted to validate access once every quarter.* ***(Completed, April 2013)***

## 3.4. Missing or Incomplete Access Management Procedures

### 3.4.A. Background and Findings

Management procedures are important within an organization to ensure that the various services use the same *modus operandi* to perform activities that meet identified business risks and, more specifically within the framework of our audit, that reduce to an acceptable level the risks associated with users' access to information systems containing PI.

For example, a procedure to manage users' access would include requirements to comply with the following elements:

- Request for access;
- Change to access;
- Review of users and their access rights;
- Deletion of access.

During our audit, we noted the following discrepancies:

- There is no access management procedure for the SDSR application;
- The access management procedure for the Employeur D application is incomplete since it does not contain a concise description of the steps to be taken when requesting the creation of access.

We estimate the impact level to be **moderate** since the city faces the following potential risks: there are missing or incomplete procedures that could lead to non-compliance with security requirements regarding access management. As a result, unauthorized individuals could have access to PI housed on Employeur D and SDSR.

### 3.4.B. Recommendation

**We recommend that the Service du capital humain et des communications (for the Employeur D system) and the Division de la gestion des programmes de logement, which reports to the Direction de l'habitation of the Service de la mise en valeur du territoire (for the SDSR system), define a procedure for managing access, which contains, at the very minimum, requirements to comply with the following elements:**

- **Request for access;**
- **Change to access;**
- **Review of users and their access rights;**
- **Deletion of access.**

**Business units' responses:**

***SERVICE DU CAPITAL HUMAIN ET DES COMMUNICATIONS***

*[TRANSLATION] Following your recommendation, the procedure was revised.* ***(Completed, March 2013)***

***SERVICE DE LA MISE EN VALEUR DU TERRITOIRE***

*[TRANSLATION] Drafting of an access management procedure for the SDSR system that provides a process to follow for access requests, amendments and cancellations, as well as for the twice yearly updating of the list of users.*

*Dissemination by email of the access management procedure to all staff at the Direction de l'habitation and storage of the documents in the computer network's common registry.*

*First update of the table of system users. This update should be done twice a year.* ***(Completed, April 2013)***

## 3.5. Discrepancies in the Physical Security of the Premises Housing Pay Records

### 3.5.A. Background and Findings

The Division de la paie institutionnelle occupies, among others, premises on the mezzanine of the Chaussegros-de-Léry building. In these premises, certain employee pay records are

filed in moveable (Rolodex-style) shelves. These records contain a large amount of sensitive PI, such as the first name, last name, address, SIN, banking information and date of birth of employees.

Based on good industry practices and in the spirit of the *Act respecting access to documents held by public bodies and the protection of personal information*, offices that contain sensitive information must be protected by containment mechanisms to prevent unauthorized physical access. These mechanisms can be, for example, an area reserved for the storage of files, or doors installed to separate hallways or other means of access, such as stairs, from the offices. These doors should be fitted with card reader access locks.

After visiting all the premises of the Division de la paie institutionnelle, we concluded that stairs, which begin in the mezzanine and are not an emergency exit route, lead to the upper floors that are occupied solely by employees of other city services. The stairs, which provide unrestricted access to the upper levels, have no containment mechanisms.

We estimate the impact level to be **moderate,** since the city faces the following potential risks: by taking the stairs, employees who are not part of the Division de la paie institutionnelle could circulate freely to the pay records in the Rolodex shelves on the mezzanine. Consequently, a malicious employee could have access to PI and steal it by consulting certain pay records.

### 3.5.B. Recommendation

**We recommend that the Division de la paie institutionnelle of the Service des finances implement security measures to restrict physical access from the stairs leading to the upper floors so that only authorized employs can access the mezzanine of the Chaussegros-de-Léry building.**

**Business unit's response:**

> *[TRANSLATION] The Division de la paie institutionnelle will move its activities to 740, rue Notre-Dame Ouest as of summer 2013. The premises will be secured by magnetic access doors.* ***(Planned completion: summer 2013)***