	Confidentiality incident management procedure **Mission Mayday**
Coming into force	September 19, 2023
Presented by	Board of Directors

1 - Confidentiality incident

The provisions contained in sections 63.8 to 63.11 of the Access Act define the concept of a breach of confidentiality and set out the procedures to which Mission Mayday complies. These articles list the criteria that the public entity concerned must take into consideration when assessing the risks of harm to an individual whose personal data is affected by a privacy breach.

2 - Communication of notifications to the Commission for Access to Information and affected parties

In the event of an incident presenting a significant risk of harm to the individuals concerned, Mission Mayday is required to immediately notify the Commission for Access to Information (CAI). Additionally, the entity must notify parties affected by the incident, unless doing so would interfere with an investigation by a person or entity authorized by law to prevent, detect, or suppress criminal activities or violations of law. . As soon as the information is no longer likely to hinder such an investigation, the public entity must promptly inform the persons concerned.

3 - Assessment of harm

In the event of a privacy breach, the public entity is required to assess whether it poses a potential risk of harm to a person whose personal data is at stake. To this end, it must take into account various elements , notably :

1. The sensitivity of personal information, such as financial data or identifying information;

2. The anticipated consequences of the use of this data, including the risk of identity theft, financial fraud or serious breaches of privacy;

3. The likelihood that this information could be used for harmful purposes.

Serious harm refers to an act or event that may cause significant damage to the person concerned or their property, having a significant impact on their interests. This can result, for example:

- Deterioration of reputation;

- A financial loss;
- Humiliation;
- Identity theft;
- Negative repercussions on the credit file;
- A job loss.

4 - Keeping a record of confidentiality incidents

Mission Mayday maintains a comprehensive record of all privacy incidents it has encountered, including those that do not pose a substantial risk of harm to the individuals involved.

The Commission for Access to Information (CAI) has the right to consult the data collected in this register, and a copy of it must be provided to it upon request.

5 - Order-making powers of the Access to Information Commission

Mission Mayday takes into account the fact that the Commission for Access to Information (CAI) holds several ordering powers in relation to confidentiality incidents.

In particular, it has the power to order:

- To a public body which has been the victim of an incident involving a serious risk of harm and which has failed to inform the persons whose personal data are affected by this incident, to inform them immediately.
- It is up to any party to put in place the necessary measures to protect the rights of those affected.
- The return of personal information involved in the confidentiality incident to the public body that held it, as well as its destruction.

The government brought into force the Regulations on Confidentiality Incidents, aimed primarily at specifying the details surrounding the notifications to be sent to the Commission d'access à l'information and to affected individuals when a confidentiality incident causes serious harm. It also specifies the content required for the register to be maintained by public entities.

6 - Privacy incident management

A. Assessment of the situation:

When Mission Mayday suspects that a confidentiality incident involving personal information has occurred, the organization takes the following steps:

- Examine the circumstances surrounding the incident;

- Identify the personal data concerned;

- Identify affected individuals;

- Diagnose the nature of the problem, whether it is an error, a security breach, or other. This assessment should continue until all relevant elements are identified.

B. Risk reduction:

Mission Mayday must respond promptly by taking reasonable steps to mitigate risks, whether serious or not, and to prevent future similar incidents. This may include actions such as:

- Put an end to any unauthorized practice;

- Recover or demand the destruction of affected personal data;

- Fix computer vulnerabilities.

C. Determination of the nature of the damage:

The objective is to establish whether notification to the Commission for Access to Information (CAI) and to the persons concerned is necessary, as well as to define the measures to be taken to reduce the risks. For example :

- Include a note in the files associated with the risks of identity theft;

- Require additional verifications.

D. Registration in the register:

Mission Mayday records the event in the incident log, whether or not it is classified as serious in terms of potential harm.

E. If there is a risk of serious harm:

- Notification to the CAI: Mission Mayday immediately informs the CAI, even if all information relating to the incident is not yet available. Mission Mayday can thus report the incident to the CAI and complete the declaration later, including the precise number of people affected.

- Notification of affected individuals: Mission Mayday notifies all individuals whose personal information is affected by the incident, unless such notification would compromise an ongoing investigation. A delay may apply between incident discovery and notification in order to gather critical information, identify affected individuals, resolve the security breach, or not interfere with an ongoing investigation. These notifications are mandatory.

F. If there is a risk of serious harm:

Mission Mayday may also notify any person or organization that can reduce this risk. For this purpose, the organization may share only the personal information necessary for this purpose, without requiring the prior consent of the person concerned. However, the Person Responsible

for Personal Data Protection must document this communication by recording the following details:

- The recipients of the information;
- The circumstances surrounding the communication;
- The specific information transmitted;
- The objectives of this approach.

Last updated: September 19, 2023