PARTENARIAT DU QUARTIER DES SPECTACLES MONTRÉAL

PROCEDURE FOR HANDLING CONFIDENTIALITY INCIDENTS

Table of Contents

1. PREAMBLE

The PQDS recognizes the importance of respecting privacy and protecting the Personal Information in its possession, as outlined in its *Policy on the Protection of Personal Information*.

To that end, the PQDS implements security measures designed to ensure the protection of Personal Information throughout its Life Cycle. These measures are designed to be reasonable given, among other things, the sensitivity of the Personal Information, the purpose for which it is used, its quantity, its location and its storage medium.

These measures are detailed in the PQDS' *Policy on Cybersecurity, Data Security and the Responsible Use of Technological Assets*.

Despite these measures, there remains a possibility of Confidentiality Incidents occurring. The PQDS has therefore adopted the present procedure for managing Confidentiality Incidents, for taking reasonable steps to reduce the risk of harm to any person, and for preventing the occurrence of further Confidentiality Incidents of a similar nature.

2. LEGAL FRAMEWORK

The present procedure is governed by articles 3.5 to 3.8 and 81.4 of the *Act Respecting the Protection of Personal Information in the Private Sector*, RLRQ c P-39.1.

3. DEFINITIONS

Capitalized terms that are not defined in the present procedure are used as defined in the PQDS' *Policy on the Protection of Personal Information*.

In addition, the following definitions apply to the present procedure:

Confidentiality Incident: the unauthorized access, use or disclosure of Personal Information, as well as the loss of a piece of Personal Information or any other lapse in its protection at the fault of the PQDS. Some examples:

- a cyberattack;
- an employee of the PQDS accesses Personal Information not required for performance of their duties;
- an employee of the PQDS accesses Personal Information to which they have legitimate access for their duties but uses the information to commit identity theft;
- a message containing Personal Information is sent to the wrong person, for example via Teams or email;
- documents or devices in the possession of a PQDS employee and containing Personal Information are lost or stolen.

Log: the log of Confidentiality Incidents.

Personal Information: any information pertaining to a physical person that can make it possible to identify the person either:

- directly, i.e. through disclosure of that single piece of information;
- indirectly, i.e. through correlation with one or more other pieces of information.

Personal Information is sensitive due to its medical, biometric or otherwise private nature, or due to the context of its use or disclosure, and thus carries a high level of reasonable expectation of privacy.

4. APPLICABILITY

The present procedure applies to all persons who commit or have knowledge of a Confidentiality Incident involving Personal Information in the possession of the PQDS, or who have good reason to believe that such an incident has occurred. In particular, it applies to:

- Employees of the PQDS;
- Any other physical or legal person, specifically members of the PQDS Board and its committees, as well as partners, consultants and vendors.

5. PROCESS FOR HANDING A CONFIDENTIALITY INCIDENT

5.1 Reporting

Any person who commits or who has knowledge of a confidentiality incident, or who has good reason to believe that such an incident has occurred, is required to report it without delay to the PQDS employee responsible for the protection of Personal Information in the following manner:

- PQDS employees: by using the form *Signaler un Incident de confidentialité* found on the PQDS employees' portal;
- All other persons, whether physical or legal: by sending an email to vieprivee@quartierdesspectacles.com.

The report must include the following information:

- Identification: the first and last names of the person filing the report, and in the case of persons who are not PQDS employees, their contact information (phone number and email address), so that they can be reached for additional information.

- Circumstances: a description of the circumstances of the Confidentiality Incident and the manner in which the person reporting it learned of it, or their good reasons to believe that such an incident has occurred, whichever applies.

- Date of the Confidentiality Incident: the date or dates during which the Confidentiality Incident occurred. If unknown, the reporter should provide an approximate date or

date range.

- Date of learning of the incident: the date on which the person reporting it discovered the Confidentiality Incident, or on which they developed good reasons to believe that an incident occurred.

- Personal Information details: the types of Personal Information affected by the Confidentiality Incident or a complete list of the Personal Information, but without reproducing the information itself in the report. If these details are unknown, the reporter should list reasons why it is impossible to provide them.

- Person(s) Concerned: the number, identity and/or category of the Person(s) Concerned whose Personal Information was affected by the Confidentiality Incident. If this information is unknown, provide an approximate number.

- Corrective and preventive measures: the report should include a description of the corrective measures taken in order to bring the Confidentiality Incident to an end, as well as the preventive measures implemented to prevent another Confidentiality Incident of the same nature.

5.2 Analysis by the PQDS employee responsible for the protection of Personal Information

a. Confidentiality Incident

Upon receiving a report, the PQDS employee responsible for the protection of Personal Information analyses the situation in order to determine whether it constitutes a Confidentiality Incident at the fault of the PQDS and records their decision in the Log. They may contact the person who filed the report in order to obtain additional information.

If the decision is that the incident is not a Confidentiality Incident as defined herein, the analysis concludes at this step.

b. Corrective and preventive measures

When handling a Confidentiality Incident, the PQDS employee responsible for the protection of Personal Information ensures that the corrective and preventive measures taken are adequate. If they are not, they provide instructions for improving the measures.

If needed, depending on the seriousness of the Confidentiality Incident, the PQDS employee responsible for the protection of Personal Information engages a third party to assist in managing the risks.

c. Risk for Persons Concerned

When a Confidentiality Incident has occurred, the PQDS employee responsible for the protection of Personal Information determines whether the Persons Concerned whose Personal Information was affected by the Confidentiality Incident are at risk of serious harm,

and records this decision, with reasons, in the Log.

To that end, the PQDS employee responsible for the protection of Personal Information considers the following elements with respect to the Personal Information affected by the Confidentiality Incident:

- Its sensitivity;
- The potential malicious uses of the Personal Information;
- The known consequences of their use (identity theft, financial fraud, significant invasion of privacy, damage to reputation, loss of employment);
- The likelihood of the Personal Information being used maliciously.

Personal Information in the following categories is generally considered sensitive: financial, genetic, biometric, health, sexual orientation, ethnic origin, race.

5.3 Notification of the Confidentiality Incident

a. When there is a risk of serious harm

When a Confidentiality Incident presents a risk of serious harm, the PQDS employee responsible for the protection of Personal Information is required to advise the Commission d'accès à l'information du Québec and the Persons Concerned who are affected by the Confidentiality Incident. They enter these communications in the Log.

Nevertheless, the PQDS employee responsible for the protection of Personal Information is not required to notify a Person Concerned if doing so would interfere with an investigation being conducted by a person or organization that is legally obligated to detect or take action against crimes or other legal infractions.

The person responsible may also advise any person or organization that may be capable of reducing the risk, sharing only the Personal Information required for this purpose without notifying the Persons Concerned. The PQDS employee responsible for the protection of Personal Information must enter such communications in the Log.

b. When there is no risk of serious harm

When a Confidentiality Incident does not carry a risk of leading to serious harm, the Commission d'accès à l'information du Québec is not advised of the incident.

The PQDS employee responsible for the protection of Personal Information may, at their discretion, advise the Persons Concerned affected by the Confidentiality Incident, especially for transparency reasons. The person responsible enters such notifications and reasons in the Log.

c. Infraction or crime

When the PQDS employee responsible for the protection of Personal Information has good reason to believe that the Confidentiality Incident constitutes or results from a legal infraction or a crime, they contact the police.

d. The Board

Depending on the seriousness of the Confidentiality Incident, the PQDS employee responsible for the protection of Personal Information notifies the Board. For purposes of the present article, a Confidentiality Incident is serious when it is caused by a cyberincident or carries a risk of serious harm. A cyberincident is any attempt, successful or not, to obtain unauthorized access to a computing resource or network belonging to the PQDS, including any attempt to modify, destroy, erase or disable it.

5.4 Confidentiality Incidents Log

For each Confidentiality Incident, the Log contains the following information and documents:

- The first and last names of the person who filed the report;
- The circumstances;
- The date of the incident;
- The date of discovery of the incident;
- The affected Personal Information;
- The affected Persons Concerned;
- Corrective and preventive measures taken;
- Confirmation of details by the PQDS employee responsible for the protection of Personal Information;
- Presence or absence of risk of serious harm to the Persons Concerned, and the nature of the potential harm;
- The dates and methods used to notify the Commission d'accès à l'information du Québec and the Persons Concerned, as well as any communications.

The Log also contains entries for reports that the PQDS employee responsible for the protection of Personal Information has deemed not to constitute Confidentiality Incidents, with reasons for reaching this conclusion.

The Log is maintained by the PQDS employee responsible for the protection of Personal

Information. It is confidential and only persons authorized by the PQDS employee responsible for the protection of Personal Information are allowed to access it.

6. PUBLICATION AND UPDATES

The present procedure is published on the website of the PQDS. The PQDS may update it from time to time in order to ensure compliance with laws related to the protection of Personal Information, or to improve procedures and practices in this area.

7. COMMUNICATIONS

All questions concerning the present procedure must be submitted by email to the PQDS employee responsible for the protection of Personal Information:
vieprivee@quartierdesspectacles.com.