

Client list in a US-hosted CRM

Example Distribution

Person in charge of the protection of personal information
Julien Example, President

Project
Client list in a US-hosted CRM

Project type
Acquisition or development of an information system

Date
September 25, 2026

Version
1

In-depth

Level of review

5

Findings

2 gaps, 3 to confirm

0

Priority risks

high severity and likelihood

1

Vendors outside Québec

5

Measures

1 Purpose and scope

Example Distribution, a distributor with 25 employees, is replacing the spreadsheet that holds its client list on the office server with a customer relationship management (CRM) application offered online by an American vendor. The project aims to centralise client records and sales history in one place and to help staff follow up on quotes and reminders. The records concern the contact persons at each client, between 100 and 10,000 persons in all, as well as the employees who use the application.

This assessment covers the personal information that will be held in the CRM: the names and contact details of client contact persons, their purchase history, the free-text notes written by sales representatives, and the names and email addresses of employees who use the CRM. It looks at how this information is collected, hosted by the vendor, accessed internally, retained and returned. The information is not intended for any purpose beyond the two described, and the project does not involve any decision made exclusively by automated processing. The assessment does not extend to other systems or activities of Example Distribution.

Under the fourth paragraph of section 3.3 of the LPRPSP, the assessment is proportionate to the sensitivity of the information, the purposes of its use, its quantity, its distribution and the medium on which it is stored. On those factors, this assessment is carried out at a high level of detail.

- LPRPSP: Act respecting the protection of personal information in the private sector (CQLR, c. P-39.1).

2 Personal information concerned

Information	Nature	Persons concerned
Name and contact details of contact persons	Contact details	Clients
Purchase history	Behaviour or preferences	Clients
Free-text notes by sales representatives	Other	Clients
Name and email of the employees who use the CRM	Employment	Staff

Factor (s. 3.3)	Finding
Sensitivity	medium
Purpose	Centralise client records and sales history; Follow up on quotes and reminders
Quantity	100 to 10,000 persons
Distribution	At least one processing outside Québec

Factor (s. 3.3)	Finding
Medium	Cloud

3 Data flows

Personal information about client contact persons originates with the clients themselves and with the sales representatives who deal with them. It includes names and contact details, purchase history, and notes that representatives type freely in a text field. Because that field has no set limits, it sometimes contains personal details unrelated to sales, such as the fact that a contact person is on sick leave. Whether the persons concerned are informed that their information is collected and held in this way remains to be confirmed. The names and email addresses of the employees who use the CRM are also recorded in the application.

The information is hosted and processed by the CRM vendor in the United States. Example Distribution accepted the vendor's online terms without reading them, so whether a written agreement governs how the vendor protects and uses the information remains to be confirmed. Inside Example Distribution, all sales and customer service staff can see every record, whether or not they deal with the client concerned.

No retention period has been defined for the records, so the information stays in the CRM indefinitely for now. What the application returns to Example Distribution is a centralised view of client records and sales history, along with follow-ups on quotes and reminders. Whether the information can be retrieved from the vendor in a structured, commonly used format remains to be confirmed.

Example Distribution



OUTSIDE QUÉBEC

CRM vendor

Hosting and processing of client records

United States · Written agreement: Does not know

Processing	Vendor	Location	In Québec	Written agreement
Hosting and processing of client records	CRM vendor	United States	No	Does not know

4 Findings and risks

Findings

To confirm

LPRPSP, ss. 17 and 18.3

No written agreement with CRM vendor, outside Québec

Section 17 requires that a communication outside Québec be the subject of a written agreement that takes the results of the assessment into account. Section 18.3 requires that the mandate or contract be in writing and specify the protection measures the vendor must take.

Answer: does not know

Gap

LPRPSP, s. 20

Access not limited to staff who need it

Section 20 makes information accessible within the enterprise only to staff who are qualified to know it and for whom it is necessary to perform their duties.

Answer: no

Gap

LPRPSP, ss. 23 and 3.2

No retention period defined

Section 23 requires destroying or anonymising information once the purposes of its collection are achieved, and section 3.2 requires policies governing its retention and destruction.

Answer: no

To confirm

LPRPSP, s. 8

Persons concerned not informed

Section 8 requires informing the person concerned, when the information is collected, of the purposes, the means and their rights, and where applicable of the third parties it is communicated to and of the possibility that it be communicated outside Québec.

Answer: does not know

To confirm

LPRPSP, s. 3.3

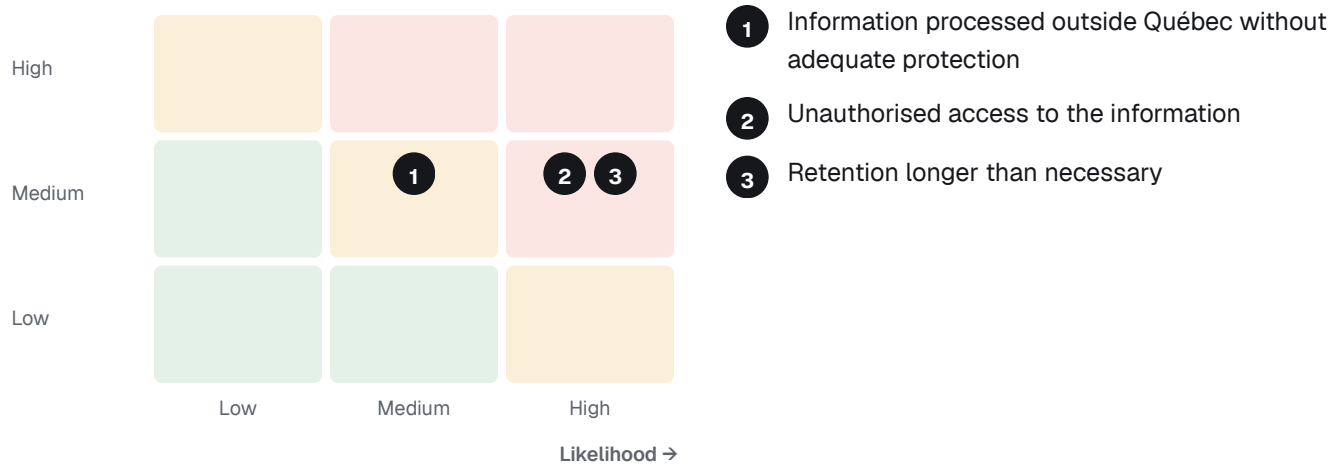
No communication in a structured format

Section 3.3 requires that the project allow computerised information collected from the person concerned to be communicated to them in a structured, commonly used technological format.

Answer: does not know

Risks

Severity ↑



#	Risk	Severity	Likelihood	Sections
1	Information processed outside Québec without adequate protection	medium	medium	LPRPSP, s. 17
2	Unauthorised access to the information	medium	high	LPRPSP, ss. 20 and 10
3	Retention longer than necessary	medium	high	LPRPSP, s. 23

5 Communication outside Québec

CRM vendor - United States

Factor (s. 17)	Finding
1. Sensitivity of the information	medium
2. Purposes of its use	Hosting and processing of client records
3. Protection measures, including contractual ones	Written agreement: Does not know
4. Legal framework of the State	The United States has no general federal privacy law. Protection varies by state and by sector, and government access regimes are broader than in Québec. These points describe the legal framework; they do not conclude that it is adequate.

The organisation's conclusion (to complete): section 17 allows the communication if the assessment establishes that the information would receive adequate protection, and requires a written agreement.

6 Measures adopted

The measures below follow from the characteristics of the project. For each one, the organisation states whether it is in place or planned, and who is responsible.

	In place	Planned	Responsible
Determine the purposes before collecting, and collect only the information necessary for them. LPRPSP, ss. 4 and 5	☐	☐	_____
Take reasonable security measures given the sensitivity, purposes, quantity, distribution and medium of the information. LPRPSP, s. 10	☐	☐	_____
Sign a written agreement with each vendor outside Québec that takes the results of this assessment into account. LPRPSP, s. 17	☐	☐	_____
Inform the persons concerned, at collection, that their information may be communicated outside Québec. LPRPSP, s. 8	☐	☐	_____

	In place	Planned	Responsible
Set out the procedure for confidentiality incidents, and record each incident in the incident register. LPRPSP, ss. 3.5 and 3.8	☐	☐	

7 Conclusion

The assessment brought to light five findings about the move to the CRM. No written agreement with the vendor, which processes the information outside Québec, has been confirmed. Access is not limited to the staff who need it. No retention period is defined. Whether the persons concerned are informed, and whether their information can be communicated in a structured format, remains to be confirmed. From these findings, three main risks emerge: information processed outside Québec without adequate protection, unauthorised access to the information, and retention longer than necessary. The last two are considered likely. The free-text notes field adds to these risks because it can hold personal details, including health-related ones, that serve no purpose in the project.

Several points remain to be confirmed, notably the content of the vendor's terms that Example Distribution accepted without reading them, and whether the persons concerned have been informed. Example Distribution adopts the five measures set out in this document to address the findings and risks identified.

This document was drafted from the organisation's answers. It applies the cited provisions to those answers and does not constitute legal advice. The organisation adopts it under the responsibility of its person in charge of the protection of personal information.

Adoption

The organisation adopts this assessment and the measures it sets out.

Name: Julien Example

Title: President

Date:

Signature:

Appendix: the organisation's answers

Question	Answer
Project type	Acquisition or development of an information system
Purposes	Centralise client records and sales history; Follow up on quotes and reminders
Use for a new purpose	No
Quantity	100 to 10,000 persons
Medium	Cloud
Retention period defined	No
Access limited to staff who need it	No
Decision based exclusively on automated processing	No
Human review of the decision	No
Identification, location or profiling technology	No
Product offered to the public with privacy settings	No
Collection from minors under 14	No
Persons concerned informed	Does not know
Communication in a structured format possible	Does not know
Person in charge consulted from the start	Yes