OSLER

Completing the Law 25 puzzle: insight into the right to data portability

SEPTEMBER 20, 2024 7 MIN READ

Related Expertise

- Artificial Intelligence
- French Language Laws
- Privacy and Data Management
- Risk Management and Crisis Response

Authors: Catherine Labasi-Sammartino, Maryna Polataiko, Andy Nagy, Katelyn Smith, François Joli-Coeur

Starting September 22, 2024, the final Law 25 amendments to the *Act Respecting the Protection of Personal Information in the Private Sector* (the *Québec Privacy Act*) will expand individual access rights. Notably, individuals will have the right to request that an organization provide them with computerized personal information collected from them in a structured, commonly used technological format. Individuals also will be able to request that an organization provide this information to another person or organization authorized to collect the information.

Osler's National Privacy and Data Management team have prepared this Update to help organizations prepare for the last set of changes brought on by Law 25 by clarifying key aspects of this new data portability right while taking into account recent guidance issued by the Québec government on the equivalent right to data portability in the public sector and the Québec privacy regulator, the *Commission d'accès à l'information* (CAI), regarding this legislative change in the private sector.

Amendments to section 27 of the *Québec Privacy Act* coming into force on September 22, 2024, are underlined:

Every person carrying on an enterprise who holds personal information on another person must at the request of the person concerned, confirm the existence of personal information, communicate it to the person and allow him to obtain a copy of it.

At the applicant's request, computerized personal information must be communicated in the form of a written and intelligible transcript.

Unless doing so raises serious practical difficulties, computerized personal information collected from the applicant, and not created or inferred using personal information concerning him, must, at this request, be communicated to him in a structured, commonly used technological format. The information must also be communicated, at the applicant's request, to any person or body authorized by law to collect such information.

If the person concerned is handicapped, reasonable accommodation must be provided on request to enable the person to exercise the right of access provided for in this division.

Scope of a data portability request

The scope of data portability requests is limited to "computerized personal information collected from the applicant". This notably means that the following information would be out of scope:

- non-computerized (i.e., a paper format) personal information
- personal information collected from third parties or sources other than the individual directly (noting that the CAI and the Québec government consider that information collected indirectly from individuals is in scope e.g., purchase or travel history)
- data "created or inferred using personal information concerning" an individual (e.g., user profiles created from web activity analysis or the use of algorithms)[1]

Conversion to an acceptable 'data portable' format

In response to a data portability request, organizations must share the requested information in a structured, commonly used and technological format. While Québec's privacy laws do not explicitly define the terms "structured," "commonly used" and "technological", recent publications from the Québec government and the CAI suggest that "structured" and "commonly used" refer to open and interoperable formats that can be easily recognized, extracted and processed by widely available software. Formats that are difficult to extract, or require proprietary or paid licenses, are generally considered unsuitable for data portability purposes.

The Québec government has specifically recommended file formats like CSV, XML and JSON as suitable for data portability requests. In contrast, the Québec government has stated that formats such as images and PDFs do not meet such requirements for data portability.[2]

It is worth noting that guidance from the Québec government clearly instructs organizations to accommodate individuals if they request that their information be provided in a specific format, unless doing so would present serious practical difficulties.

Communication of information to an authorized third party

Organizations must not only provide the information in a data portable format to the individual themselves but also, upon request, to any person or body authorized by law to collect such information. The term "authorized by law" indicates that the data recipient (i.e. the entity receiving the information in a portable format) must comply with the legal obligations that govern its collection of personal information, in accordance with the applicable privacy legal framework.

According to the Québec government, a data recipient is considered "authorized by law" to collect the information only if the following conditions are met:

- Public bodies: If the data recipient is a public body under the *Act respecting access to documents held by public bodies and the protection of personal information* (the *Québec Access Act*), the collection must be "necessary" for the exercise of the body's functions or the implementation of a program under its management.[3]
- Enterprises: If the data recipient is an enterprise under the *Québec Privacy Act*, the

collection must be for a "serious and legitimate" reason and "necessary" for the purposes identified prior to collection.[4]

- Other recipients: If the data recipient is neither a public body nor an enterprise, the collection must be for a "serious and legitimate" reason and "relevant" to the stated objective of the file.[5]

Notably, the Québec government indicates that there is an obligation for the entity handling a request to transfer information in a data portable format to verify that the third party recipient is legally authorized to collect the information before granting the request. This may involve additional steps, such as establishing written procedures and assessing the recipient's reasons for data collection to ensure they comply with legal requirements.

However, CAI guidance for the private sector does not explicitly require the disclosing organization to perform due diligence. Instead, it places the responsibility on the receiving organization to assess the necessity of the information it receives. This shift of responsibility to the recipient aligns with the right to data portability's goal of facilitating easier transitions for individuals between service providers. As such, the specific obligations for both the recipient and the disclosing organizations remain unclear.

Nonetheless, the CAI emphasizes that disclosing organizations must implement appropriate security measures when sharing personal information in a structured, commonly used and technological format. Although specifics have not been provided, one can easily imagine that these measures may include encryption and secure file transfer protocols.

Response to a data portability request

Since the right to data portability is an extension of the right of access, organizations receiving a request for data portability must follow the *Québec Privacy Act* rules governing responses to access requests. For example, organizations must verify that the individual making the request is the person to whom the personal information relates or is their representative, heir or successor, person having parental authority, or other person authorized by law to access the information, as applicable.[6] Organizations must also respond no later than 30 calendar days after the date the request is received (subject to limited exceptions).[7] In cases where a request is denied, organizations must also assist the applicant in understanding the refusal, if requested.[8]

Note that non-compliance with data portability obligations is not explicitly subject to fines or penalties. However, the CAI has broad order-making powers that could require the organization to take corrective action if refusal to grant the request for data portability was, in whole or in part, determined to be unfounded.[9] Failure to comply with such orders may lead to further enforcement actions, including possible penalties.[10]

Refusal of a request due to 'serious practical difficulties'

Organizations receiving a valid data portability request concerning information that is not already held in a data portable format must convert the information into a structured, commonly used and technological format, unless doing so raises "serious practical difficulties." According to the Québec government, such difficulties may result from particularly high costs or the complexity of the information transfer required. Any organization invoking "serious practical difficulties" must be prepared to provide necessary

justifications during a potential review by the CAI.

Project involving the processing of personal information

Under the *Québec Privacy Act*, any organization launching a new project for acquiring, developing, or overhauling an information system or electronic service involving personal information must conduct a privacy impact assessment (PIA) and must ensure that computerized personal information collected from the individual can be provided to them in a structured, commonly used and technological format.[11] For example, to meet this requirement, the Québec government suggests offering features such as allowing individuals to download their information. Other compliance strategies might also include integrating data export functionalities into user interfaces and ensuring that third-party systems are compatible with commonly used formats for data transfer.

Key steps to compliance

Key steps for compliance with the new data portability right include

- identifying information within the scope of the right to data portability
- ensuring that the identified information can be shared in a structured, commonly used and technological format
- updating internal policies and procedures to include the handling of Québec data portability requests
- reviewing external policies and notices to ensure individuals are informed of the right of access and how they may exercise this right
- updating PIA templates to include a section on data portability, as applicable
- if denying a data portability request due to "serious practical difficulties," documenting the specific reasons for the refusal

Additional Law 25 resources, including a detailed data portability checklist, are available for AccessPrivacy subscribers. Visit AccessPrivacy to learn more.

---

1. These examples are taken from the guidance published by the Québec government and the CAI. ↩
2. The United Kingdom's Information Commissioner's Office has published guidance on the Right to data portability in the context of the U.K. GDPR, which includes useful discussion on the meaning of "structured" and "commonly used" formats. ↩
3. Section 64 of the Québec *Act respecting Access to documents held by public bodies and the Protection of personal information* (*Québec Access Act*). ↩
4. Sections 4–5 of the *Québec Privacy Act*. ↩
5. Article 37 of the *Civil Code of Québec*. ↩
6. Section 30 of the *Québec Privacy Act*. ↩

7. Sections 32 and 46 of the *Québec Privacy Act*. □□
8. Section 55 of the *Québec Privacy Act*. □□
9. Section 91 of the *Québec Privacy Act*. □□
10. Section 34 of the *Québec Privacy Act*. □□
11. Section 3.3 of the *Québec Privacy Act*. □□