Québec Law 25 still has more to say: Answers to your questions on the new data portability right

August 09, 2024

The last part of Law 25, the "right to data portability", will come into force in Québec on Sept. 22, 2024, in the *Act respecting the protection of personal information in the private sector* (Private Sector Act) and the *Act respecting access to documents held by public bodies and the protection of personal information* (Access Act).

This date also marks the end of the one-year leniency period following the entry into force of the main components of this major legislative reform, as informally announced by the Commission d'accès à l'information (CAI). With Québec's regulator now expected to be more proactive in enforcing the law, what do you need to know to implement this new individual right?

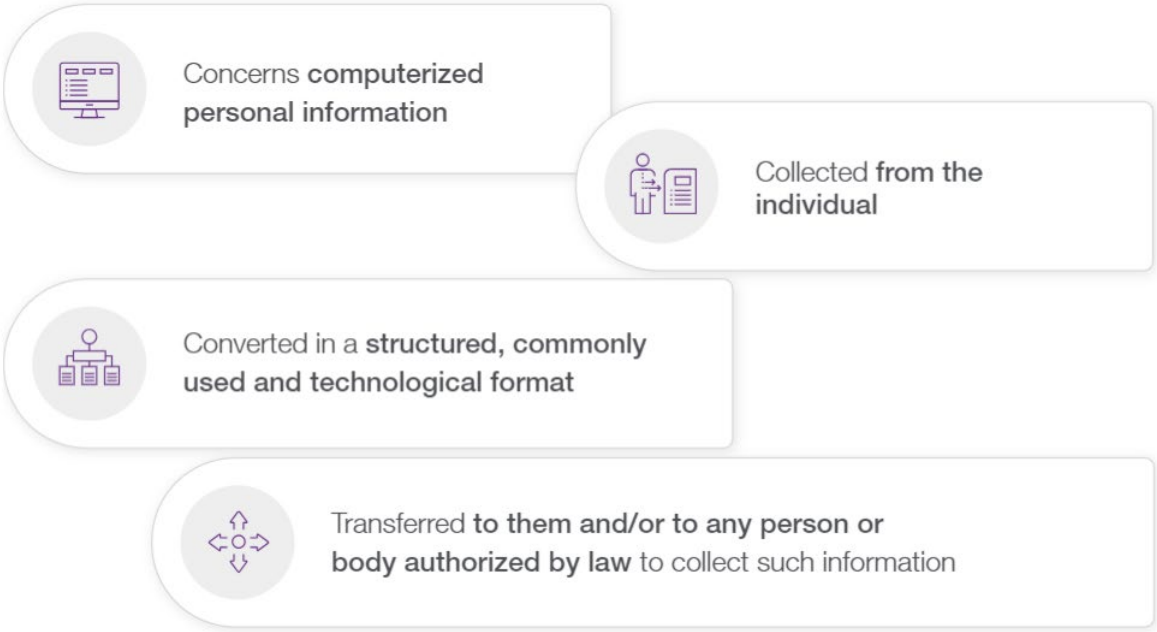
What is the right data portability?

The right to data portability introduced in Québec is part of an international trend to give consumers more power and control over their data and, at the same time, to increase competition between businesses.[1]

In Law 25, it is the new section 27 (3) of the Private Sector Act (section 84 (3) Access Act) that introduces data portability in the form of a technological and enhanced variant of the right of access:

> **27.**
>
> 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 the 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 his 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. […]**

In short, Québec's right to data portability can be summed up as follows:



Let us look in detail at what these elements imply.

To which information does the right to data portability apply?

A valid data portability request must relate to (i) computerized personal information that (ii) has been collected by the organization from the person concerned directly.

- **Computerized Personal Information**

  The term "computerized personal information" refers to personal information held on a medium that uses information technology.[2] This excludes information collected in paper format only.

  This can include information that has been uploaded by the individual to an electronic file, as well as information generated by the individual's online activity such as their shopping or travel history.

- **Information collected by the organization from the person directly concerned**

  Information collected by the organization from the person concerned includes information provided directly by the individual, or information collected automatically using certain technologies such as surveillance cameras and audio recordings.

The right to data portability therefore does not apply to the following:

- **Personal information collected from third parties**, such as a business partner, a service provider, or even a public database (e.g., the Québec Enterprise Register).
- **Personal information created or inferred by the organization** from the individual's personal information, such as a consumer profile or credit score. This exemption protects certain confidential informational assets whose disclosure could result in the loss of a competitive advantage for the organization.[3]

What is the appropriate format for data portability?

To comply with the right to data portability, an organization must provide computerized personal information in a format that is:

- **technological;**
- **structured; and**
- **commonly used.**

An organization may respond to a data portability request by directly transferring the requested information to the individual (or authorized third party), or by providing access to an automated tool that allows the individual to retrieve the requested information themselves (for example, think of a customer's online account).

The notion of "structured and commonly used technological format" is not explicitly defined in Québec legislation. However, given the undeniable influence of the European Union's *General Data Protection Regulation* (GDPR) on Law 25, the interpretation of the right to data portability under the GDPR may provide some food for thought. For example, the former Article 29 Working Party issued guidelines defining the right to portability as:

'[...] a set of minimal requirements that should facilitate the interoperability of the data format provided by the data controller. In that way, "structured, commonly used and machine readable" are specifications for the means, whereas interoperability is the desired outcome.'

On its French-only website, France's data protection authority, the Commission nationale de l'informatique et des libertés (CNIL), says that open formats such as CSV, XML and JSON are best adapted to data portability, with metadata proving useful to assist comprehension. On the other hand, a format that is difficult to process, such as an image, a PDF or a format whose use involves the acquisition of software or a paid license, are not, a priori, formats suitable for the exercise of that right.

The choice of the appropriate format for responding to a portability request is entirely up to the organization processing the request.

Can one of our employees make use of this right?

Yes, this right is available to anyone about whom an organization holds personal information, including its own employees.

What is the time limit to respond to a data portability request?

A business must process a data portability request within 30 days of receipt (section 32 Private Sector Act) while a public body has 20 days, subject to a notice of extension of up to 10 days (section 98 Access Act).

If the organization fails to respond to the request within the required time limit, it is deemed to have refused the request.

The time limit within which an organization must process a data portability request may be extended provided that a request is submitted to the CAI before the original time limit expires (section 46 of the Private Sector Act/section 137.1 of the Access Act). Unlike other Canadian privacy laws, there is no limit in Québec on the total number of days by which the CAI may extend the time limit.

Is it necessary to verify the identity of the applicant?

The organization must verify the identity of the applicant (section 30 Private Sector Act / section 94 Access Act). In accordance with the requirements of the right of access, a data portability request may be considered only if it is made in writing by a person proving their identity as:

- a person concerned;
- the representative, heir or successor of that person;
- the liquidator of the succession;
- a beneficiary of life insurance or of a death benefit;
- a person having parental authority, even if the minor child is deceased; or
- the spouse or a close relative of the deceased person.

Which third parties are authorized to receive the information following a data portability request?

The person concerned may request that their computerized personal information be disclosed to any person or body authorized by law to collect such information. However, the law does not specify whether the third party must rely on a particular provision of a law authorizing it to collect that information or whether the consent of the applicant is sufficient. Until proven otherwise, the concept of "authorized third parties" must therefore be interpreted broadly.

In addition, the extent of the obligation of the organization processing the portability request as to the lawfulness of the collection of the information by the third party indicated by the applicant remains uncertain. In our view, the organization must exercise a minimum of diligence to ensure that the information will not be used for malicious purposes. It should be noted that the organization remains responsible for personal information in its custody or control. This could result in the business breaking the law and being held liable if it transfers personal information to an unauthorized third party, in cases where there is fraud or identity theft, for example.

When is it possible to refuse a data portability request?

The right to data portability, like the right of access it complements, is not absolute.

An organization that receives a request under this right may refuse to disclose it for the following reasons:

- **In the presence of serious practical difficulties**

Where the provision of information in a structured and commonly used technological format raises serious practical difficulties for the organization receiving the request, the latter may be exempted from the requirement to comply with this requirement. In particular, such difficulties may result from the significant costs and/or complexity involved in transferring the information to the appropriate format or to a third party. An organization invoking such a ground must be able to demonstrate these difficulties if the request were ever to be reviewed by the CAI.

- **If a restriction on the right of access applies**

As portability is an extension of the right of access, the provisions that allow the organization to refuse access to certain information (sections 37 to 41 Private Sector Act / sections 86 to 88.1 Access Act) are applicable. This will be the case, for example, where disclosure of the information would be likely to reveal the identity, and cause serious harm, to a third party who has not consented to it, or affect ongoing legal proceedings (section 40 Private Sector Act / section 88 Access Act).[4]

- **If the request is obviously abusive**

The current and unchanged version of section 46 of the Private Sector Act (section 137.1 Access Act) allows organizations to refuse portability if the requests are obviously unfounded or excessive, including because of their repetitive, systematic or inconsistent nature with the purpose of the law, provided that they obtain authorization from the CAI.

When the request is refused, the organization's Privacy Officer must respond in writing, state the reasons for the refusal, indicate the provision on which the refusal is based (if applicable), and inform the applicant of the remedies available to them as well as the time limit for exercising them (section 34 Private Sector Act / section 50 Access Act). On the latter point, the organization must inform the applicant of their right to submit a request for an examination of a disagreement to the CAI within 30 days of the refusal to grant the request. Upon request, the Privacy Officer must also help the applicant to understand the reasons for the refusal.

An organization that refuses to grant a portability request must also retain the information for the time required to allow the individual to exhaust the remedies provided by law (section 36 Private Sector Act / section 52.1 Access Act).

If the request for portability has been refused or if it has not been processed within the time limit provided by law, the applicant may file a request for examination of a disagreement or a request for review with the CAI (section 42 Private Sector Act / section 135 Access Act).

Is it possible to charge a fee to process a data portability request?

Reasonable fees may be charged for the transcription, reproduction or transmission of information (section 33 Private Sector Act / section 85 Access Act). Note, however, that the fees charged may be challenged before the CAI. An organization that intends to charge a fee must inform the applicant of the approximate amount payable before proceeding with the transcription, reproduction or transmission of that information.

In practice, what do I need to do to ensure that my organization will be able to process a data portability request?

The first step is to review your existing processes for handling access requests to ensure that the specific requirements of this right are properly integrated. For example, your internal policies and standards should provide examples of the computerized information that may be covered, specify the formats that may be used, establish criteria for determining whether a third party is authorized to receive information, etc.

In addition, any organization should also:

- **Identify the data covered**

Some personal information is more likely to be the subject of such a request. To identify it, ask yourself what information would make it easier for one of your customers to transition to your competitor.

- **Clarify the limits of your organization's responsibility**

Consider having applicants sign a document clarifying the limits of your organization's responsibility versus that of the one that receives the information. If your organization transfers information, the individuals involved must understand that you will no longer control how a customer's data is used. Conversely, if you are to receive information pursuant to a portability request, make it clear to the applicant that you are not liable for any errors or inaccuracies in the data you receive.

- **Determine what security measures apply**

If your organization is facing a significant volume of portability requests, make sure your information security teams are involved to ensure that communication to third parties follows established security standards.

- **Review your external privacy policy**

As with other individual privacy rights, a business's external privacy policy plays a key role in directing your customers to your internal procedures. Greater transparency on how to exercise this right will allow you to centralize and simplify the processing of the resulting requests.

The imminent entry into force of the right to portability should remind businesses of the need to have procedures for responding to the many individual rights conferred by this law. While the remaining obligations under Law 25 have come into force in recent years, there is still time to ensure your business's compliance as the leniency period observed by the CAI draws to a close.

Contact us

BLG's Cybersecurity, Privacy and Data Protection group closely monitors legal developments that can strategically inform organizations on Canada's data protection requirements. If your organization has questions about the right to data portability in Québec, please reach out to the key contacts below or any other member of our group.

Footnotes

[1] See, for example, article 20 of the *General Data Protection Regulation* within the European Union, and article 1798.130(3)(b)(iii) of the *California Consumer Privacy Act* in the United States. In federal Bill C-27, the *Consumer Privacy Protection Act* (C-27), the right to "mobility of personal information" is provided for in section 72.

[2] In our view, the concept of computerized personal information can be reconciled with that of a technological document provided for in the *Act to establish a legal framework for information technology*, RLRQ v. C-1.1, s. 3 (4).

[3] See the exchanges during the parliamentary debates on Bill 64 on this subject (in French only).

[4] For more information, see BLG, *Managing access requests: A decision by the Commission d'accès à l'information provides valuable insights for organizations*.

By

Simon Du Perron, Frédéric Wilson, Cléa Jullien

Expertise

Cybersecurity, Privacy & Data Protection

BLG | Canada's Law Firm

As the largest, truly full-service Canadian law firm, Borden Ladner Gervais LLP (BLG) delivers practical legal advice for domestic and international clients across more practices and industries than any Canadian firm. With over 725 lawyers, intellectual property agents and other professionals, BLG serves the legal needs of businesses and institutions across Canada and beyond – from M&A and capital markets, to disputes, financing, and trademark & patent registration.

blg.com

BLG Offices

Calgary

Centennial Place, East Tower
520 3rd Avenue S.W.
Calgary, AB, Canada
T2P 0R3

T 403.232.9500
F 403.266.1395

Ottawa

World Exchange Plaza
100 Queen Street
Ottawa, ON, Canada
K1P 1J9

T 613.237.5160
F 613.230.8842

Vancouver

1200 Waterfront Centre
200 Burrard Street
Vancouver, BC, Canada
V7X 1T2

T 604.687.5744
F 604.687.1415

Montréal

1000 De La Gauchetière Street West
Suite 900
Montréal, QC, Canada
H3B 5H4

T 514.954.2555
F 514.879.9015

Toronto

Bay Adelaide Centre, East Tower
22 Adelaide Street West
Toronto, ON, Canada
M5H 4E3

T 416.367.6000
F 416.367.6749