

# Data localization



## Things to know

- Private sector privacy laws permit organizations in Canada to transfer personal information to another jurisdiction for processing, but does impose conditions.
- Public sector privacy laws in some provinces (British Columbia and Nova Scotia) prohibit personal information in the custody or control of public bodies from being stored or accessed outside of Canada, subject to exceptions.
- In some circumstances, health information laws prohibit personal information from being disclosed outside of a province or Canada.

## Things to do

- Before transferring personal information, assess the risks to the integrity, security and confidentiality of the data outside of Canada – this may require avoiding transfers to certain countries or transferring sensitive information.
- Obtain contractual commitments from any service provider (including affiliated companies) so that the personal information will have comparable protections to the protections in Canada.
- Inform individuals that their information may be sent to another country and may be accessed by the courts, law enforcement and national security authorities under local laws (which may be different than the laws in Canada).
- Ensure that you do not store or access personal information (e.g., when providing a digital or cloud service) on behalf of a public body, hospital or health provider without considering how geographic restrictions found in Canadian legislation may apply.

### USEFUL RESOURCES

- [Guidelines for Processing Personal Data Across Borders](#)

### RELATED TOPICS

- [Consumer privacy](#)
- [Mobile app privacy](#)
- [Human rights in the workplace and privacy](#)



### Need more info?

Osler's Privacy team can help. Find out more at [osler.com/dataprivacy](https://osler.com/dataprivacy)