Treasury Board of Canada Secretariat
Secrétariat du Conseil du Trésor du Canada
Canada

Direction for Electronic Data Residency

Published: 2018-06-25

Published by Treasury Board of Canada, Secretariat
90 Elgin, Ottawa, Ontario, K1A 0R5, Canada

Catalogue Number: BT22-210/2018E-PDF
ISBN: 978-0-660-26558-2

This document is available on the Government of Canada website, Canada.ca

This document is available in alternative formats upon request.

Aussi offert en français sous le titre : Orientation relative à la résidence des données électroniques

Government of Canada | Gouvernement du Canada

Direction for Electronic Data Residency

From Treasury Board of Canada Secretariat

IT Policy Implementation Notice (ITPIN (Information Technology Policy Implementation Notice))

ITPIN (Information Technology Policy Implementation Notice) No:

2017-02

Date:

November 1, 2017

Updated:

March 13, 2018

The purpose of this ITPIN is to direct departments and agencies on the control, access and ownership of Government of Canada (GC) electronic data.

This ITPIN is effective as of November 1, 2017, and all initiatives, procurements, projects and services that require the storage and/or transmittal of Protected B, Protected C and classified GC electronic data must be in full compliance with this ITPIN as of the effective date. All existing initiatives, procurements, projects and services requiring the storage or transmittal of Protected B, Protected C and classified GC electronic data that are not in full compliance with this ITPIN as of the effective date must be reported immediately to Treasury Board Secretariat, Chief Information Officer Branch, along with a plan to bring the initiative, procurement, project or service into full compliance with this ITPIN. The Government of Canada Chief Information Officer has the sole authority to grant exemptions to this ITPIN.

This ITPIN applies to departments as defined in section 2 of the Financial Administration

Act unless otherwise excluded by other acts, regulations or orders in council.

The heads of the following organizations are solely responsible for monitoring and ensuring compliance with this ITPIN within their organizations:

- Office of the Auditor General
- Office of the Chief Electoral Officer
- Office of the Commissioner of Lobbying of Canada
- Office of the Commissioner of Official Languages
- Office of the Public Sector Integrity Commissioner of Canada
- Offices of the Information and Privacy Commissioners of Canada

Background

The GC stores and moves its electronic data through distributed computing networks and GC-approved computing facilities located both within Canada and internationally. The location and movement of the data is subject to various international, national or local laws and regulations.

Data residency refers to the physical or geographical location of an organization's digital information while at rest.

As discussed in the Government of Canada Cloud Adoption Strategy, the growing use by the GC of cloud computing services has and will continue to amplify issues relating to the applicability of foreign laws to Canada's data and issues relating to Canada's ability to maintain continuous access to its data.

In the context of cloud computing, keeping data resident within Canada is intended to maintain, to the greatest extent possible, the GC's continuous access to Protected B, Protected C and classified data that is vital to the GC's business continuity, including the delivery of key services to Canadians, such as the payment of Employment Insurance and Canada Pension Plan benefits, the flow of goods across Canada's border, and the security screening of passengers at airports, including the screening of individuals arriving in Canada. Specifically, when the data physically resides in Canada, it is subject to the protections afforded by Canadian privacy laws and Canada will be better situated to take prompt action, for example, in the event that access to data is compromised. Keeping data resident in Canada is also important for safeguarding sensitive information in the interest of national security.

Direction

All sensitive electronic data under government control, that has been categorized as Protected B, Protected C or is Classified, will be stored in a GC-approved computing facility located within the geographic boundaries of Canada or within the premises of a GC department located abroad, such as a diplomatic or consular mission. This does not mean that the country of origin of IT service providers must be Canada, as long as these service providers can ensure storage of data within boundaries or premises as described above.

All Protected B, Protected C and classified GC electronic data in transit must be encrypted when in transit outside of GC controlled Operations and Security Zones within Canada or internationally.

Departments must ensure that a risk-based approach is used for verifying and monitoring the supplying entity's compliance with GC security requirements, as identified in GC policies, standards, and expressed in contracting documentation, before authorization is granted for these facilities to process, store, or transmit Protected B, Protected C and classified GC electronic data.

Depending on the level of sensitivity of the information, departments may need to implement additional measures to protect information on electronic media and electronic storage devices at rest, in addition to the residency requirements defined in this ITPIN.

Direction for Electronic Data Residency, ITPIN No: 2017-02 must be used for the implementation of GC electronic data residency safeguards. The ITPIN supports the Policy on the Management of Information Technology, 2007.

Requests for exemptions from this ITPIN must be submitted to the Treasury Board Secretariat, Chief Information Officer Branch (CIOB- ITD email mailbox) with a rationale to justify the request.

Definitions

A GC-approved computing facility is located within the geographic boundaries of Canada or within the premises of a GC department located abroad, such as a diplomatic or consular mission, and provides the GC unimpeded access to and control over GC electronic data. Such a facility can be either owned and/or managed by the GC or a non-GC entity.

Classified electronic data is data that if compromised would reasonably be expected to cause an injury to the national interest. This includes all data that falls within the exemption or exclusion criteria under the Access to Information Act and the Privacy Act. Data described in the exclusion criteria is deemed to be important either to preserving the

national interest or to protecting other interests for which the government assumes an obligation. This also includes data that has regulatory or statutory prohibitions and controls.

Protected B and Protected C electronic data is data that, if compromised, could cause serious or extremely grave injury to an individual, organization or government.

It is also important to recognize that large collections of information require greater security measures than single documents classified at any given level. For further details see Levels of Security.

References

- Access to Information Act, 1985
- Privacy Act, 1985
- Policy on Access to Information, August, 2014
- Policy on Government Security, April, 2012
- Policy on Management of Information Technology, July, 2007
- Policy on Privacy Protection, August, 2014
- Government of Canada Information Technology Strategic Plan 2016-2020, June, 2016
- Government of Canada Cloud Adoption Strategy, July, 2016
- Information Management Manual, Office of the Information Commissioner of Canada (PDF, 203 KB), 2010
- Directive on Departmental Security Management, 2009

Please address any inquiries you may have by email to the CIOB-DPPI IT-Division-TI.

Marc Brouillard
Chief Technology Officer of the Government of Canada
Chief Information Officer Branch
Treasury Board of Canada Secretariat

ISBN: 978-0-660-26558-2

Date modified:

2018-06-25