Techrupt

Checklist

Canadian Data Residency Checklist for BC Organizations

What FIPPA, PIPA and PIPEDA mean for your Azure and Microsoft 365 environment, and how to prove compliance

Techrupt Digital, Microsoft Solutions Partner

Updated September 2026

How to use this checklist

Use this checklist for the joint review between your privacy office and your cloud team. Privacy decides what the law and your contracts require. The cloud team shows, with evidence, that the environment does what the privacy impact assessment (PIA) says it does.

Work through the sections in order, then use the master checklist at the end as the summary sheet for a PIA or audit file. Every item has a yes, no or not applicable answer. A "no" is either a gap to close or an exception to document.

This checklist describes Techrupt Digital's consulting approach. It is not legal advice. Confirm your obligations with your privacy officer or legal counsel.

Which law applies to you

For most BC organizations, no law says data must stay in Canada. BC public bodies lost that requirement in 2021, when FIPPA amendments replaced it with a risk assessment. Private organizations under PIPA or PIPEDA have never had a general residency rule, but they stay accountable for what they send abroad, and a client contract can still impose one.

Organization type	Primary law	Residency position
BC public body: ministry, health authority, school district, municipality	FIPPA	No blanket rule since 2021. Sensitive personal information stored outside Canada needs a supplementary assessment in the PIA.
BC corporation, not-for-profit, charity, trade union or credit union	BC PIPA	No general residency rule.
Federally regulated business, such as a bank or telecom, or data crossing provincial or national borders	PIPEDA	No general residency rule. Transfers need contractual protection and notice to individuals.
Vendor processing data for a public body	Contract, plus PIPA or PIPEDA	The client's residency clause is usually the binding constraint.

- [ ] The privacy office has confirmed the governing law for each system in scope
- [ ] Client and vendor contracts are checked for residency or data location clauses
- [ ] The result is recorded in the PIA or system security plan, not only in email

FIPPA obligations for BC public bodies

The FIPPA amendments received royal assent on November 25, 2021. They removed the restrictions on storing information outside Canada and strengthened PIA requirements in their place. Three provisions now carry the weight.

Section 33.1. A public body may disclose personal information outside Canada only in accordance with the regulations, if any, made by the minister.

B.C. Reg. 294/2021. The head of a public body must assess any program, project or system in which sensitive personal information is disclosed to be stored outside Canada, as part of the PIA. Programs that existed when the regulation took effect are exempt, as is information made public under section 33(2)(f).

Section 69. Every public body must conduct PIAs in accordance with the minister's directions. Ministries document the supplementary assessment in the PIA. Other public bodies may choose their own format.

FIPPA does not define "sensitive personal information". Provincial guidance treats it as a question of type and context, with health, financial, biometric and criminal records as common examples.

Section 30 still requires reasonable security arrangements. The Office of the Information and Privacy Commissioner (OIPC) says disclosure outside Canada demands a very high level of rigour, and its factors include whether a reasonable alternative exists in Canada. With two Canadian Azure regions available, a PIA that stores health data in a US region has to explain why the Canadian option was not reasonable.

- [ ] Every system in scope has a current PIA
- [ ] Sensitive personal information is identified in each system's data classification
- [ ] Any sensitive personal information stored outside Canada is identified
- [ ] A supplementary assessment is completed for each such disclosure, or the exemption relied on is recorded
- [ ] The PIA explains why a Canadian alternative was not reasonable, where data leaves Canada
- [ ] Section 30 security arrangements are documented for each system

PIPA and PIPEDA for private organizations

The federal Office of the Privacy Commissioner (OPC) lists BC's PIPA as substantially similar to PIPEDA. PIPEDA still applies to federally regulated businesses and to personal information that crosses provincial or national borders.

The OPC's cross-border guidance is explicit that PIPEDA does not prohibit transfers for processing. The transferring organization stays accountable. It must use contracts to secure a comparable level of protection and tell individuals their information may be processed in another jurisdiction.

In practice, residency reaches the private sector through contracts. A company that processes data for a health authority usually inherits that client's residency clause.

- [ ] Every service provider that handles personal information is listed
- [ ] Contracts with those providers require a comparable level of protection
- [ ] Privacy notices say where information may be processed outside Canada
- [ ] Residency commitments made to clients are enforced in Azure, not only stated

Azure region choices

Microsoft runs two Azure regions in Canada, and they are paired with each other.

	Canada Central	Canada East
Location	Toronto	Quebec City
Availability zones	3	None listed
Paired region	Canada East	Canada Central
Service breadth	Broader	Narrower; check each service
Typical role	Primary production region	Disaster recovery and backup target

Because the pair sits inside the Canada geography, geo-redundant storage (GRS) replicates to Quebec City rather than to a US region. A region pair does not give you disaster recovery by itself. You still design and test failover.

The design we usually recommend for BC clients: production in Canada Central across availability zones, replication to Canada East for disaster recovery, and a check before sign-off that every service in the design exists in both regions. Canada East lacks some services and SKUs.

- [ ] Production workloads run in Canada Central or Canada East
- [ ] Each service and SKU in the design is confirmed available in both Canadian regions
- [ ] Storage accounts using GRS or GZRS are confirmed to replicate to the Canadian pair
- [ ] Azure SQL active geo-replication targets are confirmed, since they can point to any region
- [ ] Failover is designed and tested, not assumed from the region pair

Microsoft 365 data location basics

Microsoft 365 works differently from Azure. You do not pick a region per resource. The country entered when the tenant was created sets its Default Geography, which Microsoft states cannot be changed afterwards. Services provision data based on that geography.

Canada is a Local Region Geography, with Microsoft 365 data at rest stored in Toronto and Quebec City. For Canadian tenants, the Product Terms carry a data location commitment for Exchange Online, SharePoint and OneDrive, Microsoft Teams, and Microsoft 365 Copilot and Copilot Chat. The Advanced Data Residency (ADR) add-on extends commitments to further services, including Microsoft 365 web apps, Defender for Office P1, Viva Connections and selected Purview services.

Not every service is deployed in Canada. Microsoft's own example is Forms, which is deployed only in the Americas and European Union/EFTA macro regions, and the Americas region includes US data centers. Microsoft also notes that a request may be handled by servers outside your region because of network routing, without data moving at rest.

You can see where core services store your data in the Microsoft 365 admin center under **Settings > Org settings > Organization profile > Data location**.

- [ ] The Data location card shows Canada for Exchange, SharePoint, OneDrive and Teams, with a screenshot on file
- [ ] Other Microsoft 365 services in use are checked against Microsoft's data location pages
- [ ] Services without a Canadian commitment are either restricted or named in the PIA
- [ ] ADR is considered where committed residency is needed beyond the core services
- [ ] Copilot use is included in the PIA, based on its documented data location

Enforcing residency in Azure

A residency decision that lives only in a PIA will drift. The control that holds up in audits is Azure Policy, assigned at the management group so every current and future subscription inherits it. This belongs in the landing zone from day one.

Use two built-in definitions together:

- **Allowed locations** (`e56962a6-4747-49cd-b67b-bf8b01975c4c`) denies resources outside the regions you list.
- **Allowed locations for resource groups** (`e765b5de-1225-4ba3-bd56-1ac6695af988`) covers resource groups, which the first policy skips.

```
# Deny any resource outside the two Canadian regions, for every subscription under the management group
az policy assignment create \
    --name "allowed-locations-canada" \
    --display-name "Allowed locations: Canada only" \
    --policy "e56962a6-4747-49cd-b67b-bf8b01975c4c" \
    --scope "/providers/Microsoft.Management/managementGroups/<mg-id>" \
    --params '{"listOfAllowedLocations": {"value": ["canadacentral", "canadaeast"]}}'
```

Two limits matter. The built-in definition excludes resources in the "global" region, so non-regional services pass straight through. And it checks where a resource lives, not where a service processes data.

- [ ] Allowed locations is assigned at management group scope with Canada Central and Canada East only
- [ ] Allowed locations for resource groups is assigned at the same scope
- [ ] No subscription sits outside the management group hierarchy
- [ ] Both assignments have enforcement mode set to Default, not DoNotEnforce
- [ ] A compliance report for both assignments is exported and kept as evidence
- [ ] Resources in the "global" region are inventoried and reviewed separately

Services that can process data outside Canada

Region policy controls where a resource lives. It does not control where every service processes data. Microsoft Entra ID is non-regional and may store identity data globally for most geographies. Azure CDN and Front Door cache content at edge locations worldwide. Both need to be named in the PIA as known flows.

AI deployment types are the gap we see most often. In Microsoft Foundry, a Global deployment may process prompts and responses in any geography where the model is deployed. A Data Zone deployment keeps processing inside a Microsoft-defined zone, such as the US or the EU, and none of those zones is Canada. Data at rest stays in the resource's geography in both cases. Only a Standard (regional) or regional provisioned deployment keeps inference in Canada.

The trap is that a Foundry resource in Canada Central passes the Allowed locations policy while a Global deployment underneath it sends prompts elsewhere. Microsoft documents a custom policy that denies deployments by SKU name, such as `GlobalStandard`. Assign it next to the location policy for any workload that handles personal information.

- [ ] Non-regional services in use are listed in the PIA with the data they handle
- [ ] Edge caching is excluded for content containing personal information
- [ ] Every AI model deployment is inventoried with its deployment type
- [ ] A SKU deny policy blocks Global and Data Zone deployments for workloads with personal information
- [ ] Regional model availability in Canada is confirmed before the design is approved

Documenting exceptions for a PIA

Some workloads will need a service or region outside the policy. That is acceptable when the exception is deliberate, approved and time-bound.

In Azure, record exceptions as policy exemptions rather than by removing or narrowing the assignment. An exemption has a category (Mitigated, when the policy intent is met another way, or Waiver, when non-compliance is temporarily accepted) and can carry an `expiresOn` date. When that date passes, Azure stops honouring the exemption but keeps the object for the record.

For each exception, the PIA or its appendix should record the following.

Field	What to record
System and data	The workload and the classes of personal information involved
Service or region	What falls outside Canada and why
Data flow	At rest, in processing, or both
Canadian alternative	Why a Canadian option was not reasonable
Safeguards	Encryption, access controls, contract terms
Approver	A named person with authority to accept the risk
Expiry	The date the exception ends or must be reviewed
Azure reference	The policy exemption name and category

- [ ] Every exception is recorded as a policy exemption, not by editing the assignment
- [ ] Each exemption has a category, an expiry date, and a named approver in its description or metadata
- [ ] Each exemption maps to a documented entry in the PIA
- [ ] Expired exemptions are reviewed and either renewed with approval or closed

Master checklist

Legal basis

- [ ] Governing law confirmed for each system (FIPPA, PIPA, PIPEDA or contract)
- [ ] Client and vendor contracts checked for residency clauses
- [ ] Sensitive personal information identified in each system

FIPPA public bodies

- [ ] Current PIA for every system in scope
- [ ] Supplementary assessment completed for sensitive data stored outside Canada
- [ ] Exemptions relied on are recorded
- [ ] Section 30 security arrangements documented

PIPA and PIPEDA organizations

- [ ] Service provider contracts require comparable protection
- [ ] Privacy notices disclose processing outside Canada, where it occurs

Azure regions

- [ ] Workloads in Canada Central or Canada East
- [ ] Services and SKUs confirmed in both regions
- [ ] Storage and database replication stays in Canada
- [ ] Failover designed and tested

Microsoft 365

- [ ] Data location card shows Canada for core services, with a screenshot on file
- [ ] Services without a Canadian commitment restricted or named in the PIA
- [ ] Copilot data location included in the PIA

Enforcement

- [ ] Allowed locations and its resource group variant assigned at management group scope and enforced
- [ ] Compliance report exported and kept as evidence
- [ ] "Global" region resources reviewed separately

Processing outside Canada

- [ ] Entra ID, CDN and Front Door flows documented
- [ ] AI deployments inventoried by type
- [ ] SKU deny policy for Global and Data Zone deployments where personal information is involved

Exceptions

- [ ] Every exception is a policy exemption with category, expiry and approver
- [ ] Every exemption maps to a PIA entry
- [ ] Exception register reviewed on a schedule

How Techrupt can help

Techrupt Digital is a Metro Vancouver Microsoft Solutions Partner. We work with BC public bodies and regulated organizations to build Azure landing zones where residency is enforced in policy and the evidence a privacy officer needs is available on request. That includes management group design, Allowed locations and AI deployment policies, exemption tracking, and the data flow documentation that feeds a PIA.

If you want your current environment checked against this list, you can book a free consultation at https://techrupt.io/consulting-session-booking. More on our Azure work is at https://techrupt.io/azure-consulting-vancouver.

Sources

- BC government, Data Residency Changes (2021 FIPPA amendments): https://www2.gov.bc.ca/assets/gov/british-columbians-our-governments/services-policies-for-government/information-management-technology/information-privacy/resources/2021-amendments/foippa_amendments_data_residency.pdf
- Freedom of Information and Protection of Privacy Act, BC Laws: https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/96165_03
- Personal Information Disclosure for Storage Outside of Canada Regulation, B.C. Reg. 294/2021: https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/294_2021
- BC government, Guidance on disclosures outside of Canada: https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/privacy/privacy-impact-assessments/guidance-on-disclosures-outside-of-canada
- OIPC BC, guidance on disclosure outside Canada (March 2022): https://www.oipc.bc.ca/guidance-documents/3646
- OIPC BC, For private organizations: https://www.oipc.bc.ca/for-private-organizations/
- OPC, Provincial laws that may apply instead of PIPEDA: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/prov-pipeda/
- OPC, Guidelines for processing personal data across borders: https://www.priv.gc.ca/en/privacy-topics/airports-and-borders/gl_dab_090127/
- Microsoft Learn, Azure regions list: https://learn.microsoft.com/azure/reliability/regions-list
- Microsoft Learn, Azure region pairs: https://learn.microsoft.com/azure/reliability/regions-paired
- Microsoft Learn, Azure Policy built-in definitions: https://learn.microsoft.com/azure/governance/policy/samples/built-in-policies#general
- Microsoft Learn, Azure Policy exemption structure: https://learn.microsoft.com/azure/governance/policy/concepts/exemption-structure

- Microsoft Learn, Data residency for non-regional services: https://learn.microsoft.com/azure/azure-government/documentation-government-overview-wwps#data-residency
- Microsoft Learn, Foundry deployment types: https://learn.microsoft.com/azure/ai-foundry/openai/how-to/deployment-types
- Microsoft Learn, Microsoft 365 data residency overview and definitions: https://learn.microsoft.com/microsoft-365/enterprise/m365-dr-overview
- Microsoft Learn, Where your Microsoft 365 customer data is stored: https://learn.microsoft.com/microsoft-365/enterprise/o365-data-locations