Privacy Scorecard

A simple self-assessment tool measuring digital trust and identity services against Canada's federal, provincial, and territorial privacy commissioners' joint expectations. This scorecard is a learning tool to help you explore privacy principles. It is not a compliance checklist or legal advice. Use it to spark conversation, explore unfamiliar concepts, and identify areas worth digging into further.

Source: FPT Joint Resolution (Sept 2022)
Time Required: 15–20 minutes
Best For: Digital trust and identity service providers, relying parties

How to Use this Tool
Rate your service against each question. Be honest. This simple tool reveals gaps before regulators or users do. Document evidence for each rating, then focus improvement efforts on your lowest-scoring principle.

Scoring Scale
3 – Fully implemented
2 – Partially implemented
1 – In progress
0 – Not implemented

1. Voluntariness: Adoption must be genuinely voluntary, with equivalent non-digital alternatives available without penalty.

Architecture: Do equivalent non-digital pathways exist without degraded service quality? __ / 3

Policy: Are staff trained to offer non-digital alternatives without discouraging their use? __ / 3

User Experience: Are digital and non-digital options presented with equal prominence? __ / 3

Ecosystem: Do your relying parties also maintain non-digital alternatives? __ / 3

Subtotal: __ / 12

2. Data Minimization: Systems must collect only the information necessary for each transaction

Architecture: Can users share only specific attributes required (e.g., “over 19” without birthdate)? __ / 3
Policy: Have you documented the specific purpose requiring each data element you collect? __ / 3
User Experience: Can users see exactly what information is requested before sharing? __ / 3
Ecosystem: Do you require relying parties to justify their data requests? __ / 3

Subtotal: __ / 12

3. Anti-Tracking: Digital trust and identity must not enable tracking individuals across services.

Architecture: Is the credential issuer technically prevented from knowing when/where credentials are used? __ / 3
Policy: Do agreements with partners prohibit building tracking capabilities? __ / 3

User Experience: Can users verify that their credential uses cannot be linked across services? __ / 3
Ecosystem: Have you assessed whether combined ecosystem services could enable correlation? __ / 3

Subtotal: __ / 12

4. Security: Robust measures must protect against unauthorized access and misuse.

Architecture: Is sensitive data processed on-device rather than transmitted to central servers? __ / 3
Policy: Has your system received independent security certification or audit? __ / 3

User Experience: Will affected users be notified promptly if a breach occurs? __ / 3

Ecosystem: Have you identified and addressed the weakest security points in your ecosystem? __ / 3

Subtotal: __ / 12

5. Transparency: Individuals must understand how their information is collected, used, and disclosed.

Architecture: Can users access logs of how their credentials have been used? __ / 3

Policy: Do stated policies accurately reflect actual data practices? __ / 3

User Experience: Have you tested whether typical users actually understand your disclosures? __ / 3
Ecosystem: Can users understand data flows across the full ecosystem, not just your portion? __ / 3

Subtotal: __ / 12

6. Accessibility: Systems must be equitably accessible to all Canadians.

Architecture: Does your system meet WCAG 2.1 AA accessibility standards? __ / 3

Policy: Are people with disabilities involved in your design and testing? __ / 3

User Experience: Is your service available in both official languages? __ / 3

Ecosystem: Have you identified populations excluded from your ecosystem and developed alternatives? __ / 3

Subtotal: __ / 12

7. Independent Oversight: Appropriate oversight mechanisms must ensure accountability.

Architecture: Can independent auditors verify your privacy claims? __ / 3

Policy: Do you publish regular reports on privacy performance, including incidents? __ / 3

User Experience: When users raise concerns, do they receive timely, meaningful responses? __ / 3

Ecosystem: Have you identified oversight gaps in your ecosystem and advocated for resolution? __ / 3

Subtotal: __ / 12

Calculate Your Results

1. Voluntariness __ / 12
2. Data Minimization __ / 12
3. Anti-Tracking __ / 12
4. Security __ / 12
5. Transparency __ / 12
6. Accessibility __ / 12
7. Independent Oversight __ / 12

Total: __ / 84

Above 80% - Strong Alignment. Maintain standards and address remaining gaps.
60-80% - Meaningful progress. Prioritize your lowest-scoring principles.
Below 60% - Significant gaps. Consider whether services should continue without improvement.