

CHECKLIST | FREE RESOURCE

Client Data and AI Safety Checklist

Who it is for	Owners and managers who hold customer information and use, or plan to use, AI tools
What you will get	Check that you know what customer information you hold, who can see it, and how AI tools are used with it.
Time needed	About 30 minutes

This checklist is general guidance in plain language. It is not legal advice, and it does not tell you what the law requires of your business. Privacy rules in Canada include Alberta's Personal Information Protection Act and the federal PIPEDA. Some sectors, such as health care, have extra rules. Ask a privacy professional about your own situation.

Know your data

- ☐ We have a list of the types of personal information we hold, such as names, emails, addresses, and health or financial details.
- ☐ We know where each type is stored, including spreadsheets, email and cloud tools.
- ☐ We collect only what we need, for a purpose we can state.
- ☐ We know how long we keep each type and when we delete it.

Access

- ☐ Each person has their own login. Nobody shares passwords.
- ☐ People can only see the information they need for their job.
- ☐ Multi-factor sign-in is on for email, finance and any tool that holds customer data.
- ☐ Access is removed the same day someone leaves.

AI tools

- ☐ We have a short written rule on which AI tools staff may use.
- ☐ Staff do not paste customer personal information, health information or confidential contracts into AI tools we have not approved.
- ☐ For each AI tool, we have read in its own terms where it processes data and whether it keeps or trains on what we submit.
- ☐ A person reviews AI-written content before it goes to a customer.
- ☐ We are able to tell customers when AI helps with their request.

Suppliers and software

- ☐ We keep a list of software providers that handle customer information.
- ☐ We have read how each one stores and protects that information.
- ☐ We know where they process data, including outside Canada.

If something goes wrong

- ☐ One person is named to lead the response to an incident.
- ☐ Staff know to report a suspected breach straight away.
- ☐ We know who to ask about when a breach must be reported. In Alberta, a breach with a real risk of significant harm must be reported to the Privacy Commissioner.
- ☐ We keep a record of incidents and what we did.

How to read your score

Count your ticks and find your range.

0 to 6 ticks	Start with the first section. You cannot protect information until you know what you hold and where it is.
7 to 14 ticks	You have good habits. Focus on the AI tools and Suppliers sections if you use cloud software or AI.
15 to 20 ticks	You are well organized. Review this list every six months and when you add a new tool.

Next step

Need help putting this into practice? Talk to NEXORA about setting up tools with sensible access and approval steps. For legal questions, speak to a privacy lawyer.

Talk to NEXORA: growth@nexorayyc.io | nexorayyc.io/contact

Prepared by NEXORA TECHNOLOGIES Corp., Calgary, Alberta. Free to use and share inside your own business. This is general guidance, not legal, financial or professional advice.