Ontario Bill 194: What Employers Need to Know and Why It Matters Everywhere

A New Era of Privacy and Cybersecurity in Ontario

In early 2025, Ontario quietly passed legislation that could reshape the way public-sector employers manage data, technology, and even artificial intelligence. Known as **Bill 194, the Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024**, the law introduces new obligations that go well beyond the familiar privacy rules most institutions already live with.

If you're in the Ontario public sector—whether in a ministry, a hospital, a university, or another provincial institution—this legislation should be on your radar right now. But even if you're running a private company in Ontario, or you're an employer in another province entirely, Bill 194 carries important lessons. It signals where regulation is heading: **tighter oversight of personal information, mandatory privacy impact assessments, stronger breach reporting, and new rules around the use of AI.**

This isn't just a compliance exercise. At its heart, Bill 194 reflects a growing public demand for trust. In an age where news about data breaches and AI misuse travels fast, governments and employers alike are under pressure to show they're not only compliant with the law, but also serious about safeguarding the people they serve and employ.

What Exactly Does Bill 194 Do?

To understand the impact, you need to know that Bill 194 works on two tracks. First, it amends Ontario's long-standing **Freedom of Information and Protection of Privacy Act (FIPPA)**, which governs how public institutions handle personal information. Second, it creates a brand new statute—the **Enhancing Digital Security and Trust Act (EDSTA)**—that gives the government new authority over cybersecurity, digital tools, and the use of artificial intelligence in public bodies.

At the FIPPA level, the law makes it explicit that institutions must take "reasonable steps" to safeguard personal information. That may sound obvious, but moving it into the statute gives it more weight and makes it easier for regulators to hold institutions accountable. It also introduces a new requirement that before an institution starts collecting or using personal information, it must prepare a **written privacy impact assessment (PIA)**. These assessments aren't optional—they need to spell out the purpose of the collection, how the data will be used, how it will be safeguarded, and what risks might exist. If the use of that information changes in a significant way, the PIA has to be updated.

Bill 194 also tightens breach reporting. Institutions now need to evaluate incidents against a "real risk of significant harm" standard. When that threshold is met, they must report the breach to the Information and Privacy Commissioner and often notify affected individuals as well. For the first time, annual reporting will also require institutions to publicly disclose how many breaches or losses they've experienced.

The second track, EDSTA, is less about personal information and more about the broader ecosystem. It empowers the Ontario government to issue directives and regulations requiring public bodies to adopt cybersecurity programs, manage risks, provide oversight of AI tools, and even disclose publicly when AI is being used in service delivery. In other words, the province is creating a framework that not only addresses today's concerns about data, but also looks ahead to the risks that artificial intelligence may bring into public decision-making.

Why Should Employers Care?

If you're running a provincial institution in Ontario, the compliance burden is obvious. You'll need new policies, systems, and resources to prepare PIAs, to detect and report breaches, to shore up cybersecurity defenses, and to manage the risks of AI tools in your operations. This isn't the sort of thing that can be done off the side of a desk—it requires coordination across HR, IT, privacy officers, legal counsel, and leadership.

But even if you're not directly covered, the ripple effects matter. Vendors and contractors that do business with public institutions will increasingly be expected to meet the same standards, especially around cybersecurity and AI. And for private

employers, the direction of travel is clear. Bill 194 tells us that regulators are moving toward greater accountability in how organizations use personal information and technology. It's not hard to imagine similar requirements extending into the private sector in the years ahead.

Consider, for example, a university in Ontario planning to roll out an AI system to assist with admissions decisions. Under Bill 194, that university will have to conduct a privacy impact assessment that looks not only at the data collected, but also at risks of bias, fairness, and transparency in the AI's outputs. Even if your organization isn't legally required to do the same today, it's a powerful signal. Employees, customers, and regulators are all watching closely to see how responsibly AI is used.

The Compliance Exposure

The stakes are high. Because the safeguarding duty is now explicitly in the law, institutions that fail to take reasonable steps could find themselves facing binding orders from the Information and Privacy Commissioner. In an era when reputational harm from a breach can be just as damaging as a regulatory fine, the risk is twofold.

There's also the operational cost. Preparing PIAs, running breach investigations, and building reporting systems take time, money, and expertise. For smaller institutions with tight budgets, this may feel overwhelming. Yet the alternative—being caught unprepared during an audit or after a breach—is far worse.

The cultural shift may be just as important as the legal one. By forcing institutions to prepare written assessments, to disclose breaches, and to explain their use of AI, Bill 194 is effectively making privacy and cybersecurity part of organizational culture. These aren't just IT problems anymore—they're governance issues.

What Employers Need to Do Now

If you're a public-sector employer in Ontario, the response should begin with a frank assessment. Do you currently have a process for evaluating new collections of personal information? If not, you'll need to build one quickly. Do you have a breach response plan that includes escalation, notification, and documentation? If not, you'll need to develop one before July 2025. Are you tracking where and how AI is being used in your operations? If not, you may soon be required to disclose it.

This is where cross-functional collaboration becomes essential. Privacy officers, HR leaders, IT departments, and executives will need to sit at the same table. A gap analysis is a practical starting point: where are you today, what does Bill 194 require, and what steps will close the distance? From there, institutions can prioritize. Critical systems that handle sensitive health or financial data should obviously be at the top of the list.

Training is also vital. Many breaches and compliance failures happen not because the policies weren't there, but because employees didn't understand them. Clear, repeated training—on recognizing incidents, safeguarding information, and using AI responsibly—will be a cornerstone of compliance.

Lessons for Employers Outside Ontario

You might be thinking: *This is all fascinating, but we're a private employer in Alberta—or a tech company in Quebec—and Bill 194 doesn't apply to us.* True enough,

but it would be a mistake to dismiss it.

The obligations Bill 194 imposes—stronger safeguarding, mandatory breach reporting, written privacy impact assessments, transparency around AI—are the very practices that many privacy experts believe will become the standard across Canada. In fact, federal initiatives like Bill C-27, the proposed Consumer Privacy Protection Act, are already heading in a similar direction.

Smart employers outside Ontario will take Bill 194 as a preview of what's coming. Even if you aren't legally required to prepare privacy impact assessments today, doing so builds trust with employees and customers. Even if you aren't forced to disclose AI use, being transparent about how you deploy it can reduce reputational risk. And even if you don't fall under Ontario's breach reporting rules, having a robust incident response plan is a basic best practice in an age where ransomware and phishing attacks are daily news.

Building Trust as a Competitive Advantage

At its core, Bill 194 is about trust. It's about reassuring the public that their information is safe, that technology is being used responsibly, and that institutions are accountable for their choices. For HR and compliance leaders, this presents both a challenge and an opportunity. The challenge is meeting new obligations in a way that is sustainable and integrated into day-to-day operations. The opportunity is using compliance as a way to differentiate—showing employees, customers, and partners that you take privacy, security, and fairness seriously.

Because trust is more than a legal requirement. It's a cultural asset. And in an environment where people are increasingly skeptical of institutions, it may be one of the most valuable assets an employer can have.

Final Thoughts

Bill 194 is now in effect, and more of its requirements will become binding as of July 2025. For Ontario's public institutions, the clock is ticking. But for all employers, the message is clear: the era of casual privacy practices is over. Whether through this law or others sure to follow, the expectation is rising.

Those who prepare now—not only to comply, but to embed privacy, security, and transparency into their culture—will be best positioned to thrive. Those who wait risk not only non-compliance, but also the loss of the very trust that makes workplaces resilient.