Smart glasses at work: Heads-up innovation, head-on compliance for Canadian HR & legal

January 12, 2026

Artificial intelligence is making its mark across all sectors, including in the workplace. In the past year, AI-powered smart glasses have evolved from being a novelty to becoming the focus of serious pilot programs. New product lineups have introduced enhanced AI features, fuelling enterprise trials even amid ongoing privacy debates. With advances such as lighter designs, improved microphones, and intuitive displays, these devices are driving significant gains in productivity and accessibility. However, they also present complex compliance challenges that HR and legal teams must address.

These glasses merge cameras, microphones, and real-time assistance. When worn by representatives of an employer in the course of their duties and used to capture images or audio of identifiable individuals, Canada's private-sector privacy regimes may apply to the organization's activities. In practice, that means defining a specific, necessary and transparent purpose, providing clear notice and obtaining consent, implementing appropriate safeguards, limiting retention, and honouring access rights. "Always-on" recording should be avoided; favour on-device processing where possible, and use visible indicators and signage if any recording could capture members of the public.

Employers have long worried about covert phone recordings. Smart glasses amplify both the upside and the risk. On the upside, they enable hands-free guidance and first-person documentation; on the risk side, they make unauthorized recording or cloud processing easier, and they can distract in safety-sensitive environments. A balanced policy therefore matters: spell out permitted use with visible recording indicators; prohibit covert or continuous capture; and protect confidentiality, trade secrets, and safety at all times.

Privacy first: Navigating the smart glasses frontier

It's under the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA) that organizations are first required to comply with privacy requirements in terms of purpose, notice, consent, safeguards, data detention and access rights.

Provincial laws in B.C., Alberta and Québec also apply, sometimes in place of or alongside PIPEDA, adding further layers of compliance. In practice, organizations should avoid continuous or "always-on" recording, prioritize local or on-device

processing, and use highly visible recording indicators and signage in any environment where members of the public may be present.

Employers must proactively update or draft policies to address the complex realities of real-time audio and video capture, cloud processing, and public-facing use, ensuring privacy protection keeps pace with technological innovation and regulatory expectations.

Biometrics: The bar rises nationwide

Canada's federal privacy commissioner treats all biometric data (from facial templates to voiceprints) that can uniquely identify an individual as sensitive personal information (see our September 2025 Insight), demanding documented necessity and proportionality, express consent in most cases, as well as strong safeguards and a clear prohibition on purpose creep. Be ready to offer non-biometric alternatives for workers who decline.

Québec imposes additional requirements (see our April 2022 Insight): organizations must provide prior notice to the *Commission d'accès à l'information* (CAI) when implementing biometric databases, and conduct a thorough necessity and proportionality assessment. They may face substantial penalties for non-compliance. If your application involves identification or authentication, it is advisable to proactively address these requirements and incorporate a Québec-specific addendum within your national policy framework.

Safety: Treat smart glasses like any high-distraction device

Heads-up displays and constant notifications can degrade situational awareness in transportation, warehousing, construction and other high-risk settings. Apply the same discipline you use for mobile devices: complete task-specific risk assessments; restrict use while operating vehicles or mobile equipment, whether in energized or heavy-traffic zones, at heights, or near hazardous substances unless controls demonstrably reduce risk (for example, geofencing, supervisor-enabled record-only / no-display modes, or pausing notifications).

Treat smart glasses as PPE-adjacent: confirm compatibility with hard hats, eye and hearing protection, and fall-arrest gear; prohibit use if weight, fit or cabling interferes with required PPE or line of sight; and train for "notification hygiene" so documentation capture doesn't become a distraction.

What best practices look like through a labour lens

- Start with the privacy impact assessment, but finish with a workforce plan.
- Limit use to clear, purpose-driven scenarios tied to safety, quality or accessibility.
- Adopt a smart-glasses policy that spells out notice to employees, visible recording indicators, tight retention and deletion rules, role-based access, and a favourable bias toward local/on-device processing.

- Where biometric functions are contemplated, complete a PIA, follow the Office of the Privacy Commissioner of Canada's (OPC) and CAI guidance, and obtain express consent before implementation.

That foundation gives HR and legal teams a defensible business case while letting operations test the real productivity benefits of heads-up, hands-free tools.

By staying attentive as they innovate, companies can maximize the advantages of hands-free technology while ensuring safety, privacy and compliance remain top priorities.

By

Justine B. Laurier, Danny J. Kaufer, Frédéric Wilson

Expertise

Labour & Employment, Compliance with Privacy & Data Protection, Privacy Impact Assessments (PIAs), Information Technology, Artificial Intelligence (AI)

BLG | Canada's Law Firm

As the largest, truly full-service Canadian law firm, Borden Ladner Gervais LLP (BLG) delivers practical legal advice for domestic and international clients across more practices and industries than any Canadian firm. With over 800 lawyers, intellectual property agents and other professionals, BLG serves the legal needs of businesses and institutions across Canada and beyond – from M&A and capital markets, to disputes, financing, and trademark & patent registration.

blg.com

BLG Offices

Calgary
Centennial Place, East Tower
520 3rd Avenue S.W.
Calgary, AB, Canada
T2P 0R3

T 403.232.9500
F 403.266.1395

Ottawa
World Exchange Plaza
100 Queen Street
Ottawa, ON, Canada
K1P 1J9

T 613.237.5160
F 613.230.8842

Vancouver
1200 Waterfront Centre
200 Burrard Street
Vancouver, BC, Canada
V7X 1T2

T 604.687.5744
F 604.687.1415

Montréal
1000 De La Gauchetière Street West
Suite 900
Montréal, QC, Canada
H3B 5H4

T 514.954.2555
F 514.879.9015

Toronto
Bay Adelaide Centre, East Tower
22 Adelaide Street West
Toronto, ON, Canada
M5H 4E3

T 416.367.6000
F 416.367.6749

The information contained herein is of a general nature and is not intended to constitute legal advice, a complete statement of the law, or an opinion on any subject. No one should act upon it or refrain from acting without a thorough examination of the law after the facts of a specific situation are considered. You are urged to consult your legal adviser in cases of specific questions or concerns. BLG does not warrant or guarantee the accuracy, currency or completeness of this publication. No part of this publication may be reproduced without prior written permission of Borden Ladner Gervais LLP. If this publication was sent to you by BLG and you do not wish to receive further publications from BLG, you may ask to remove your contact information from our mailing lists by emailing unsubscribe@blg.com or manage your subscription

preferences at blg.com/MyPreferences. If you feel you have received this message in error please contact communications@blg.com. BLG's privacy policy for publications may be found at blg.com/en/privacy.

© 2026 Borden Ladner Gervais LLP. Borden Ladner Gervais LLP is an Ontario Limited Liability Partnership.