Treasury Board of Canada Secretariat
Secrétariat du Conseil du Trésor du Canada
Canada

Privacy Implementation Notice 2025-01: Workplace Harassment and Violence

Published: 2025-07-07

Published by Treasury Board of Canada, Secretariat
90 Elgin, Ottawa, Ontario, K1A 0R5, Canada

Catalogue Number: BT39-87/2025E-PDF
ISBN: 978-0-660-78989-7

This document is available on the Government of Canada website, Canada.ca

This document is available in alternative formats upon request.

Aussi offert en français sous le titre : Avis de mise en œuvre de la protection des renseignements personnels 2025-01 : Harcèlement et violence en milieu de travail

Privacy Implementation Notice 2025-01: Personal information management in workplace harassment and violence occurrences

1. Effective date

This implementation notice takes effect on January 21, 2026. It replaces the notice published on July 9, 2025.

2. Authorities

This implementation notice is issued pursuant to paragraph 71(1)(d) of the *Privacy Act*.

3. Purpose

This implementation notice serves to assist government institutions in the collection, use, disclosure and retention of personal information managed as part of a workplace harassment and violence occurrence (an

occurrence). Requests for personal information or for records relating to an occurrence are also addressed.

4. Context

The process of resolving an occurrence is established in the *Work Place Harassment and Violence Prevention Regulations* (*Regulations*). These regulations are issued pursuant to the *Canada Labour Code*, Part II (the *Code*), whose purpose includes preventing occurrences of harassment and violence arising out of, linked with or occurring while at work. The *Regulations* and the *Code* establish important definitions when considering an occurrence. These include:

- principal party: an employee or employer who is the object of an occurrence
- responding party: the person who is alleged to have been responsible for an occurrence
- designated recipient: a work unit in a workplace or a person who is designated by an employer to receive a notice of an occurrence
- witness: a person who witnessed an occurrence or who is informed of an occurrence by the principal party or responding party
- employer: a person who employs one or more employees and includes an employer's organization and any person who acts on behalf of an employer; for the purposes of this guidance, it would be the federal institution

Once an employer or designated recipient has received notice of an occurrence, the resolution process begins. In accordance with section 33 of the *Regulations*, the employer must ensure that the resolution process is

completed within a year of the notice of an occurrence being provided. Section 16 of the *Regulations* requires that a notice of an occurrence must include:

- the name of the principal party and responding party (if known)
- the date of the occurrence
- a detailed description of the occurrence.

Per section 25(1) of the *Regulations*, if an occurrence is not resolved through negotiated resolution or conciliation, an investigation must be carried out if the principal party requests it.

An investigator's report sets out the following:

- a general description of the occurrence
- the investigator's conclusions on the circumstances that contributed to the occurrence
- their recommendations to minimize the risk of a similar occurrence

Subsection 30(2) of the *Regulations* sets out that the investigator's report must not reveal, directly or indirectly, the identity of the individuals involved in the occurrence or its resolution process. It is therefore written without direct or indirect personal identifiers. The report is shared with the employer or designated recipient, who, in accordance with subsection 30(3) of the *Regulations*, provides a copy of the report to:

- the principal party
- the responding party
- the workplace health and safety committee or health and safety representative

Paragraph 10(2)(h) of the *Regulations* states that the workplace harassment and violence prevention policy must describe how the privacy of individuals involved in an occurrence, or its resolution, was protected. Further requirements regarding the conduct of workplace harassment and violence

prevention and resolution are provided in the *Directive on the Prevention and Resolution of Workplace Harassment and Violence*and the *Policy on People Management*. Depending on the occurrence, other administrative or criminal investigations may occur in parallel.

5. Guidance

5.1 Collection

Paragraph 125(1)(c) of the *Code* establishes the obligations of the employer to "investigate, record and report, in accordance with the regulations, all accidents, occurrences of harassment and violence, occupational illnesses and other hazardous occurrences known to the employer." Personal information is collected throughout the process of resolving an occurrence, including during the following stages:

- the notification of an occurrence
- the negotiated resolution
- the conciliation
- the investigation

Institutions may use standard Personal Information Bank (PIB) PSE 919 Harassment for the collection of personal information throughout the resolution process. The parties involved in an occurrence will typically be employees of the government institution, but there may be cases where a party in an occurrence is an individual external to the government institution. For example, they may be a member of the public, such as a client, a family member of an employee in cases of domestic abuse, or an employee of another institution.

Under section 4 of the *Privacy Act*, no personal information shall be collected by a government institution unless it relates directly to an operating program or activity of the institution. When working to resolve an occurrence, this means that an institution may collect personal information only to the extent that it is directly related to that purpose. Direct collection requirements pursuant to subsection 5(1) of the *Privacy Act* and section 4.2.25 of the *Directive on Privacy Practices* also apply.

It is important that institutions collect only personal information that is necessary for the resolution process. During investigations, individuals might provide additional details to give context, and investigators or designated recipients might ask clarifying questions that are not directly relevant to the occurrence. Institutions can address the risk of over-collection by advising investigators and designated recipients to guide participants to limit personal information to what is directly relevant and necessary for the resolution process and in turn ensure that only this pertinent information is recorded. Institutions should also ensure that any personal information not relevant to the investigation is identified and appropriately removed or redacted.

Individuals participating in the resolution process of an occurrence must be notified about the purpose for which their personal information will be collected, in accordance with subsection 5(2) of the *Privacy Act.* As outlined in sections 4.2.20 and 4.2.21 of the *Directive on Privacy Practices*, this is to be done through a Privacy Notice Statement, which must be provided to individuals prior to the collection of their personal information. The institution’s Access to Information and Privacy (ATIP) office may assist with preparing a Privacy Notice Statement.

5.2 Use and disclosure

5.2.1 Intended use

Information collected will be used throughout the resolution process of an occurrence. Per section 4 and paragraph 7(a) of the *Privacy Act*, the collection of personal information must be limited to personal information consistent with its intended use. In this instance, the uses are resolution of the occurrence and creation of prevention and protection measures for the workplace.

5.2.2 Procedural fairness

To respect procedural fairness, and pursuant to the jurisprudence, [1] a party has the right to know and respond to evidence that contradicts their respective positions. This information may be provided through a summary of evidence, which can include personal details of the parties and witnesses where necessary. As a result, certain personal information may need to be disclosed to the parties.

5.2.3 Consistent uses of personal information

In some cases, institutions can use or disclose personal information without the consent of the individual to whom it relates. This includes consistent uses under paragraphs 7(a) and 8(2)(a) of the *Privacy Act.* For example, information shared with the employer through the resolution process can be used to initiate a separate process, such as a labour relations consultation. The information could include the notice of occurrence or interview notes and the analysis thereof. This type of sharing should be limited to specific circumstances, for example, where possible misconduct is identified. It should be noted that only the employer can use the information to initiate a separate process. Section 4.1.10.4 of the *Directive*

on Prevention and Resolution of Workplace Harassment and Violence requires that cases that involve potential misconduct be referred to a labour relations specialist to be resolved through a separate process. Initiating a separate labour relations consultation is listed as a consistent use in the Standard PIB referenced in subsection 5.1 of this document. If there is uncertainty as to whether the proposed sharing is a consistent use, government institutions are advised to consult their legal services unit before using personal information collected during an occurrence resolution process in separate labour relations consultations.

Other examples of possible consistent uses include:

- administrative investigations
- security investigations
- grievances
- disclosures of wrongdoing
- applications for judicial reviews
- civil claims
- provincial workers' compensation boards
- complaints that pertain to the *Canadian Human Right Act*

5.2.4 Safety of individuals

If there is concern for the safety of the principal party, or other employees within a government institution, information may be disclosed to security personnel, for example. Doing so may be necessary for an institution to meet its obligation as the employer to ensure workplace safety, pursuant to section 124 of the *Code*. For example, if it is suspected that a responding party, who is a member of the public, may come to the workplace and pose a threat to employees, the identity and appearance of the individual may be disclosed to the workplace's security unit. In emergency situations, personal information may be disclosed to emergency services if there is

concern for the safety of an individual or if such a disclosure would clearly benefit them. Such disclosures would be in accordance with paragraphs 8(2)(f) or (m) of the *Privacy Act*. Disclosures under 8(2)(m) can be applied only at the discretion of the head of the institution or their delegate. These 8(2)(m) disclosures must also be reported to the Privacy Commissioner in accordance with subsection 8(5) of the *Privacy Act*. For more information on disclosures pursuant to 8(2)(m) of the *Privacy Act*, consult the Office of the Privacy Commissioner of Canada's guidance on public interest disclosures.

5.2.5 Workplace assessment review

The employer may initiate a joint review and update of the workplace assessment with the workplace committee or the health and safety representative, as per paragraph 5(2) of the *Regulations*. Workplace assessments consist of identifying risk factors and developing and implementing preventive measures under sections 8 and 9 of the *Regulations*. Any information shared with the workplace committee or health and safety representative should be de-identified, as the *Regulations* emphasize that the report must be confidential.

The Privacy Notice Statement, provided during the collection, informs participants in the resolution process that there are limits to the confidentiality of the process and that their personal information could be used in other contexts, such as an investigation. If such secondary uses occur, it is a best practice to inform individuals and advise them to whom the personal information was disclosed.

5.3 Retention

Privacy officials may be consulted on the retention of personal information collected during the resolution process of an occurrence, including the applicability of certain statutory requirements to retain records.

Subsection 35(2) of the *Regulations* specifies several records that must be retained for a period of 10 years. These include:

- notices of an occurrence and action taken in response to the notices
- investigators' reports
- records of the employer's decision and reasons for that decision whenever the employer and relevant stakeholders do not agree on a joint matter
- documents that form part of each review and each update to the workplace assessment
- a document that sets out the reason for delay if a time limit set out in section 33 of the *Regulations* is not met
- annual reports
- fatality reports related to the occurrence

The correct retention period may vary for supporting documents not covered by the *Regulations*. For example, it may not be necessary to retain draft versions of the report that do not contain unique or substantive content beyond what is in the final investigator's report. Institutions should work with their information management teams to determine the correct retention periods.

It is also important to note that section 4 of the *Privacy Regulations* requires that any personal information used by a federal institution for an administrative purpose must be retained for at least two years after its last use. This could include the use of information subject to the 10-year retention period under the *Regulations*. Therefore, if the 10-year retention

period is nearing its end and the same personal information is used again, it must be kept for a minimum of two additional years beyond the original retention time frame.

When the institution hires an investigator through a contract, the third-party investigator must provide all their records to the institution so that these records may also be retained. Doing so facilitates an individual's rights of access, to request correction and to complain under the *Privacy Act*. At the same time, third-party investigators must destroy any copies in their possession, as they are no longer needed to fulfill the identified purposes or meet any legal or regulatory obligations. Institutions may require a certificate of destruction. These requirements should be included in any contracts with third-party investigators. Further guidance on privacy considerations when contracting is found in *Taking Privacy into Account Before Making Contracting Decisions*.

5.4 De-identification of reports

Collected personal information will be used to inform the investigator's report. However, as per subsection 30(2) of the *Regulations*, an investigator's report must not reveal, directly or indirectly, the identity of people who are involved in an occurrence or the resolution process for an occurrence. Therefore, the report must be written in a manner that masks all identifying features of the individuals involved. The same version of the report must be shared with all parties, who must receive a copy under subsection 30(3) of the *Regulations*. There should be no changes necessary to the report when sharing it with different parties due to the de-identified nature of the report.

The primary responsibility for de-identifying the report lies with the human resources unit, as it oversees the process and has a deeper understanding of each incident's specific context. Privacy officials may be asked to assist

with the revision of the investigator's report to ensure it is sufficiently de-identified. Because the resolution process, including the report, must be concluded within a year, there will be a firm deadline to complete such a review. Given the intricacies of these reports, vetting them for identifying information can be complex and time-consuming; therefore, it often takes longer than a straightforward *Access to Information Act* (ATIA) request of similar length. This is especially true when there are more than two parties involved in the incident. However, as exemption paragraphs do not need to be cited, privacy officials may use non-ATIP redaction software that allows for a more efficient review of the documents.

When de-identifying a report, privacy officials should consider that the report will be sent to individuals within the government institution who may have a personal relationship with the parties implicated in the occurrence, which increases the risk of re-identification. They should also consider the mosaic effect, where seemingly minor details, when combined, may reveal sensitive information. With this in mind, privacy officials should consider requesting that the investigator identify any details of the incident that they believe could identify any individual involved. This will allow the privacy officials to consider how best to redact those details and prevent re-identification of individuals. Thus, these indirect identifiers may be redacted concurrently with any direct identifiers in the report.

Guidance on de-identification and anonymization can be found in Privacy Implementation Notice 2023-01: De-identification.

5.5 Privacy protection measures for persons involved in an occurrence

Subsection 10(1) of the *Regulations* requires government institutions to develop a workplace harassment and violence prevention policy. Per paragraph 10(2)(h) of the *Regulations*, institutions must describe in their

harassment and violence prevention policies how they will protect the privacy of persons involved in an occurrence or in a resolution process. Section 4.1.9 of the *Directive on the Prevention and Resolution of Workplace Harassment and Violence* echoes this and states that appropriate measures should be taken to protect the privacy and confidentiality of all parties involved throughout the resolution process. Although this directive applies only to institutions within the core public administration, privacy obligations apply across all federal institutions. Accordingly, privacy officials in every institution should be consulted on privacy practices to protect the identity of the people involved. Standard administrative and technical safeguards should be applied to personal information. These measures will vary depending on the institution, but they could include measures such as document security markings, access controls, security training and privacy training.

The principal parties, responding parties and witnesses involved in the resolution process of an occurrence cannot be guaranteed that their involvement and personal information will not be shared publicly. Other individuals involved in the resolution process may share information about the occurrence with others, which poses a risk to confidentiality. Information may be released in response to access to information or personal information requests. Information could also be disclosed through applications for judicial review or through claims before administrative tribunals. Institutions should encourage all participants to refrain from broadly sharing information about the occurrence at their workplace. Institutions are advised to consider developing an internal policy that addresses this risk and include this consideration in the Privacy Notice Statement.

5.6 Requests for records

As noted above, per subsection 30(3) of the *Regulations*, parties to an incident must receive the investigator's report. It is the responsibility of the employer to provide a copy of the report to the principal party, the responding party, and the workplace health and safety representative. If a party has not received a copy of the report, institutions should advise them to contact their employer to request a copy of the report rather than submit an ATIP request. Even so, if an ATIP request is received for an investigator's report, it must be processed by the institution.

Individuals may request their information related to an occurrence under subsection 12(1) of the *Privacy Act* or section 4 of the ATIA. The request must provide enough detail for the institution to identify the information and allow it to reasonably retrieve the records. This is particularly important in the context of a request under the *Privacy Act*, where requestors must provide "sufficiently specific information on the location of the information as to render it reasonably retrievable by the government institution" per paragraph 12(1)(b) and subsection 13(2). Personal information that has not already been de-identified, such as raw notes or testimonies, may be reasonably retrievable and therefore responsive to a personal information request.

The measures to protect the privacy and confidentiality of the parties do not override the right to make an access request. However, institutions must apply relevant exemptions and exclusions. For example, section 19 of the ATIA or section 26 of the *Privacy Act*, which allow institutions to refuse to disclose the personal information of individuals other than the requester's, may be applied. Certain details such as who was present when the occurrence happened, what words were exchanged, or the identity of witnesses who provided their opinions on the occurrence may be redacted. However, requesters might still deduce the identity of witnesses via the

information found in their request. For example, if only one witness was present during the occurrence and information was collected from an unnamed witness, their identity may be implicit. Despite that, information that does not fall under an exemption or exclusion must be released.

If information is shared between more than one individual, a more complex analysis is required. In the decision *Canada (Information Commissioner) v. Canada (Minister of Citizenship and Immigration)*, 2002 FCA 270 (commonly referred to as the Pirie case), the Federal Court of Appeal found that responding parties can have access to limited personal information of interviewees who have provided opinions on the responding party during the investigation. In particular, the Court found that since the personal information belongs to both the interviewees and the responding party, it had to apply a balance of interest test. In doing so, the Court concluded that there was a greater interest in Mr. Pirie's right to know what had been said about him so he could appropriately exercise his right to clear his name in the department's archive pursuant to subsection 12(2) of the *Privacy Act*.

The Court found that the following personal information from interviewees who had provided opinions on the responding party could be released:

- the names of the interviewees
- information regarding their positions
- the views and opinions that the interviewees expressed about the responding party

At the same time, institutions must ensure that the disclosure of another individual's interwoven personal information is limited to only that which is strictly necessary. Such information remains subject to *Privacy Act* protections even if there are circumstances that require its disclosure.

Given the sensitive nature of an occurrence and the potential for harm to individuals, it is important that institutions take the safety of individuals into account when considering the release of information. Section 17 of the ATIA and section 25 of the *Privacy Act* may be applied where the disclosure of information could reasonably be expected to threaten the safety of individuals. This is particularly important if the principal party's personal information may be released to the responding party.

If an information request is made while an investigation is ongoing, institutions may also consider paragraph 16(1)(c) of the ATIA and paragraph 22(1)(b) of the *Privacy Act*. This includes both the investigation into the occurrence and any other investigation related to it, such as a parallel security investigation arising from the same facts. These exemptions allow institutions to refuse to disclose information if doing so could reasonably be expected to interfere with an ongoing investigation or legal proceedings. They can also be applied if disclosure could harm future investigations. To apply this exemption, the institutions must demonstrate a reasonable probability of injury by explaining the foreseeable consequences of disclosure, the potential harm and its likelihood. They must also show that disclosure was assessed based on the specific circumstances rather than by applying a broad approach.

For more information on the application of exemptions and exclusions, consult the *Access to Information Manual* and the *Personal Information Request Manual*.

6. Application

This implementation notice applies to the government institutions defined in section 3 of the *Privacy Act*, including parent Crown corporations and any wholly owned subsidiary of these corporations. However, this notice does

not apply to the Bank of Canada.

7. References

Legislation and regulations

- *Access to Information Act*
- *Canada Human Rights Act*
- *Canada Labour Code*
- *Financial Administration Act*
- *Privacy Act*
- *Privacy Regulations*
- *Work Place Harassment and Violence Prevention Regulations*

Directives and policies

- *Directive on Privacy Practices*
- *Directive on Service and Digital*
- *Directive on the Prevention and Resolution of Workplace Harassment and Violence*
- *Policy on People Management*
- *Policy on Privacy Protection*

Other

- *Access to Information Manual*
- *Personal Information Request Manual*
- Privacy Implementation Notice 2023-01: De-identification
- *Provincial and Territorial Child Protection Legislation and Policy: 2018*
- *Taking Privacy into Account Before Making Contracting Decisions*

8. Enquiries

Members of the public may contact Treasury Board of Canada Secretariat Public Enquiries for information about this implementation notice.

Employees of government institutions may contact their ATIP coordinator for information about this implementation notice.

ATIP coordinators may contact the Treasury Board of Canada Secretariat's Privacy and Responsible Data Division for information about this implementation notice.

Footnotes

1 Carreau v. Canada (Attorney General), 2025 FC 1537, Marentette v. Canada (Attorney General) 2024 FC 676, Brown v. Canada (Attorney General) 2024 FC 823.

ISBN: 978-0-660-78989-7

Date modified: 2026-03-23

xx
yy