Gap Inc. Employee Privacy Policy (Canada)

Available Languages

English Français Canada

Last Updated: November 15, 2020

I. Gap's Commitment to Protecting Employee Privacy

As global businesses, The Gap, Inc. ("Gap" or the "Company") and its affiliated entities operate in many different countries. This Policy explains how we collect, generate, use, and disclose Personal Information (as defined below) about our employees. This Policy reflects our commitment to protecting the privacy of our employees and, where applicable, our statutory obligations under provincial privacy legislation.

II. Who Is Covered by This Policy?

This Policy applies to all employees of Gap Inc. who work in Canada and/or whose Personal Information is collected, used or disclosed by Gap Inc. in Canada. Gap is committed to protecting the privacy of all individuals who work for us – in whatever capacity.

III. Who Is Accountable for Protecting Personal Information in Gap's Possession?

Gap has a Chief Privacy Officer ("CPO") who is ultimately responsible for ensuring compliance with this Privacy Policy within Canada, and for ensuring that employees' Personal Information, collected for purposes described under this Policy, is protected. The CPO may, from time to time, delegate particular responsibilities to other individuals in order to implement this Policy.

IV. What Is Considered "Personal Information"?

The majority of the Personal Information that Gap will collect, generate, use and disclose about its employees is more accurately defined as "Employee Personal Information." Employee Personal Information is the information which is reasonably necessary for the initiation, management, maintenance, and termination of the employment relationship between Gap and its employees.

For purposes of this Policy, "Personal Information" is any information, recorded or not, that is about an identifiable individual and it includes "Employee Personal Information" unless specifically excluded under this Policy.

Personal Information does not include business contact information (i.e., title, work e-mail, work phone number, etc.). It may include, but is not limited to the following categories of information:

- **Personal details**: first name and surname, work email addresses and telephone numbers, home address telephone numbers, date and place of birth, Social Insurance Number ("SIN"), marital status, dependents, emergency contact information, details and documentation required under immigration laws (such as citizenship, birth certificate, residency or work permit);
- **Professional qualifications and interests**: details contained in letters of application and résumé/CV, previous employment background, education history, professional qualifications, language and other relevant skills, personal career objectives, willingness to relocate;
- **Compensation and payroll data**: base salary or wage, bonus eligibility, benefits, pay enhancements, details on stock options and other awards, currency, pay frequency, effective date of current compensation, salary reviews and performance appraisals, banking details, working time records (including vacation/holiday schedule, sick time or other absences, hours worked and department standard hours), business expense reimbursement information, information required for statutory deductions and administration;
- **Personnel data**: hire and termination dates, terms and conditions of your contract, worker identification number, workplace address, workplace telephone number and email address, job title and function, department, business unit and location, work schedule, supervisors, appraisals, promotions, disciplinary notices, dates of absence and reasons for absence, signing authority; and
- **Sensitive information**: permitted by applicable law, such as data that identifies health-related conditions to administer benefits or provide accommodations, membership in labor unions, sex and racial or ethnic origin for diversity purposes, the commission or alleged commission of any offenses, and any proceedings for any offences alleged to have been committed and the disposition of such proceedings or the sentence of any court in such proceedings and credit information. Please be assured that, as explained in the following section, we will only use such sensitive information for appropriate purposes and as provided by law. Gap recognizes that this information is more highly sensitive and it is committed to an even higher level of privacy protection for this category of information.

An employee's social insurance number ("SIN") is also considered Personal Information. It will only be collected, used or disclosed for very limited and legislated purposes. It will never be used as a general identifier and Gap will only ask for it when there is a mandatory requirement. If it is "optional," Gap will no longer ask employees to provide their SINs.

Employees must provide Gap with emergency contact information and this information often includes Personal Information about non-Gap employees. It is the duty of all Gap employees to ensure that they have sought and received the consent of these contacts before disclosing these individuals' Personal Information to Gap.

V. Why Do We Collect, Use, and Disclose Personal Information?

We collect, generate, use and disclose Employee Personal Information without consent where it is reasonable to do so for the purpose of establishing, managing or terminating an employment relationship with an individual.

Currently, Gap collects, generates, uses and discloses Personal Information for the following purposes:

- **Managing Our Workforce.** Managing work activities and personnel generally, including appraisals, promotions and succession planning, administering salary and payment administration and reviews, wages, bonuses, employee rewards programs, providing employees with health care, pensions, training, leave, promotions, transfers, secondments, honoring other contractual benefits, as well as determining eligibility for and providing training, recreational activities, loans, stock options; reporting and carrying out workforce analysis, performing background checks, managing disciplinary actions, and terminations;
- **Communications and Emergencies.** Facilitating communication with employees at the workplace location, home and when employees are traveling; and ensuring business continuity; protecting public health, safety or property; facilitating communication in an emergency; providing references;
- **Business Operations.** Operating and managing the IT and communications systems, including company-sponsored online social networking sites, centralized email servers, marketing products or services; tracking product development; improving our products and services; managing company assets, resource allocation, strategic planning, project management; business continuity, compilation of audit trails and other reporting to promote proper business practices, budgeting, financial management and reporting, and communications within and outside the Company; managing acquisitions, mergers and re-organizations;
- **Compliance.** Complying with the Company's policies, terms of use, and legal requirements applicable to our businesses in all countries in which Gap operates, such as income tax and national insurance deductions, record-keeping, reporting obligations, and conducting audits; compliance with government inspections and other requests from government or other public authorities; responding to legal process such as subpoenas; pursuing legal rights and remedies, defending litigation and managing any internal complaints or claims arising out of or relating to employment with the Company; monitoring activities as permitted by local law (including the monitoring with regard to telephone, email, Internet, social networking sites, and other company resources).
- **Legal Authority.** As otherwise required or permitted by law.

If any additional collections, uses or disclosures of Employee Personal Information are planned, the Company will notify you of those new purposes.

To accomplish some of the purposes listed above, Gap uses a global personal information database of all employees of the Company and its Affiliates.

The Company will not collect, use or disclose Personal Information (that does not fall under the category of Employee Personal Information) for any purpose that is incompatible with the purposes outlined in this section, unless it is required or authorized by law, the employee consents to a new purpose, or is in the employee's own vital interest (e.g., in the case of a medical emergency).

VI. How Do We Collect Personal Information?

Gap will obtain consent from an employee when it collects, uses or discloses personal information about an individual employee that does not fall within the definition of Employee Personal Information, as provided for in this Policy. Circumstances where consent may not be required include but are not limited to:

- When it is required by law or to comply with a subpoena;
- When it is disclosed to assist a public body or law enforcement agency in an investigation; and
- When it is necessary to respond to an emergency that threatens the health and safety of an individual or the general public.

Gap and third parties who have access to Personal Information consistent with this policy may store and process Personal Information about employees on servers in the US and other countries that may have privacy and data security laws different from Canada's laws. Gap may need to disclose Personal Information to comply with local laws and government requests in these countries.

VII. Electronic Monitoring

Electronic Monitoring includes all forms of monitoring that is done electronically. Why and how monitoring takes place depends on what is established for an employee's roles and responsibilities.

Here are the reasons why and ways employees may be monitored. These are in addition to those set forth in Gap Inc's Electronic Communication & Social Media Policy.

Why we may monitor:

- For the safety and security of our employees and others, the protection of our premises and in the event of an investigation;
- For the purpose theft, fraud, loss prevention and to prevent illegal behavior;
- To ensure employees adhere to workplace policies, to protect legal rights, equipment, systems, and data, especially those related to the use of IT systems;
- To manage and assess performance, productivity, and related incentive programs, ensure accurate compensation, and/or adherence to working time.

How we may monitor:

- By reviewing, logging, accessing, and searching the contents of an employee's professional and permitted personal devices on Gap's systems, including telephone, email, internet (e.g., browsing history and social media networking);
- By maintaining an archive of employee activities in their use of Gap owned electronic or personal devices on Gap's systems such as email history, chat logs, phone calls, electronic work product, and text messages;
- By recording internet activities on Gap's systems (even failed attempts to access sites);

- Through the use of video technology (e.g., CCTV), of both internal (e.g., breakrooms) and external public spaces (e.g., parking lots);
- Through the use of wearable and/or handheld technology and personal tracking or motion software (e.g., bar code, magnetic stripe, RF-enabled ID badges, & ergonomics);
- By monitoring all in store and online transactions using exception-based reporting applications; and
- By monitoring the entry and exit of Gap premises via burglar alarm and access control systems.

The above-noted Electronic Monitoring may be performed at any time, without further notice, to determine compliance with this section or with any other relevant Gap policy, standard, or procedure. Any information collected by Electronic Monitoring may be used during employee reviews, for disciplinary purposes, or in connection with legal proceedings.

Should employees have any questions or concerns related to the ways or means of these electronic monitoring activities, they should contact their direct Supervisor for more information.

VIII. Do We Disclose Personal Information to Third Parties?

Gap may disclose Employee Personal Information without consent to third parties where it is reasonable to do so for the purpose of establishing, managing or terminating an employment relationship with an individual. Personal Information will only be provided to such organizations if they agree to use such information solely for the purposes for which they were originally given the information and under the instruction of Gap and, with respect to that information, to act in a manner consistent with the relevant principles articulated in this Policy.

Examples of these third parties are: Payroll providers; pension providers and/or administrators; health benefits providers and/or administrators; organizations that verify employees' employment and education background and other information provided by employees to Gap; organizations that conduct employee security checks and clearances; relocation companies; banks; workers' compensation boards and related bodies; insurance brokers; employees' treating physicians; landlords, security companies, and access card providers; Revenue and/or Tax departments; conference or training organizers or providers; schools; police and security forces.

From time to time, Gap may enter into contracts with third parties who may need to have access to the Personal Information of Gap employees. Gap will seek to include a privacy protection clause in contracts to guarantee that any third parties who will have access to Gap employees' Personal Information will provide the same level of protection as Gap.

Please note that a transfer of Personal Information within Gap is not a disclosure to a third party; however, as one of the safeguards that Gap has in place to protect employee information, Personal Information will only be transferred internally on a "need to know" basis.

IX. How Long Do We Keep Personal Information?

Gap will only retain employees' Personal Information for as long as it has a purpose to do so and/or as is required by all the applicable legislation that governs Gap's operations. Generally, an

employee's Personal Information will be maintained for as long as he or she is employed with the Company. If Personal Information has been used to make a decision that impacts an employee, that information will be kept for no less than one (1) year to allow the employee(s) reasonable time to access the information if they choose to do so. If an employee's employment is terminated for any reason, Gap will continue to retain his or her Personal Information in accordance with our Records Retention Policy or as otherwise required by law.

X. How Do We Ensure The Accuracy of Personal Information?

We endeavour to ensure that any Personal Information in our possession is as accurate, current and complete as necessary for the purposes for which we use that information. We rely on employees to ensure their Personal Information is accurate and up-to-date, particularly with respect to payroll information (i.e. bank account numbers), benefit information (i.e. dependents), background information (for security clearances) and health and medical information.

We will correct or amend any Personal Information if its accuracy and completeness is challenged and found to be deficient. We will notify the employee once the correction and/or amendment has been made.

We reserve the right to refuse to amend any information where, in our opinion, the information is accurate. If there is a disagreement between the employee and Gap with respect to the accuracy of any information, the employee has the right to indicate the specifics of the disagreement on the appropriate form or file as applicable.

We will send any information that has been amended, where appropriate, to any third parties that have access to the information.

XI. How Do We Protect and Secure Personal Information?

We will protect employees' Personal Information against loss or theft, as well as from unauthorized access, disclosure, copying, use or modification. We will protect employees' Personal Information regardless of the format in which it is held.

We will use appropriate security safeguards to provide necessary protection such as:

- Physical measures (locked filing cabinets, restricting access to offices, alarm systems);
- Technological tools (passwords, encryption, firewalls); and
- Organizational controls (security clearances, limiting access on a "need-to-know" basis, staff training, and confidentiality policies).

We will consider the following factors in selecting appropriate safeguards:

- The sensitivity of the information;
- The amount of information;
- The extent of distribution;
- The format of the information (electronic, paper, etc.); and

- The type of storage.

XII. Who Should I Talk To If I Have a Question or Concern?

Should employees have any questions or concerns related to the collection, generation, use or disclosure of their Personal Information, they should put their concerns in writing to privacy@gap.com.

Privacy Commissioners in Quebec, Alberta and British Columbia are able to investigate complaints from employees in those provinces regarding the collection, generation, use or disclosure of their Personal Information. Employees in these three provinces may file a complaint with their respective Privacy Commissioner at the following address:

Office of the Information and Privacy Commissioner (Calgary)
Suite 2460, 801 6 Avenue SW Calgary,
Alberta T2P 3W2
Phone: (403) 297-2728
Fax: (403) 297-2711
Toll Free: (888) 878-4044

Office of the Information and Privacy Commissioner for British Columbia
PO Box 9038 Stn. Prov. Govt.
Victoria, British Columbia V8W 9A4
Telephone: (250) 387-5629
Fax: (250) 387-1696
E-mail: info@oipc.bc.ca

Commission d'accès à l'information du Québec
Bureau 1.10
575, rue Saint-Amable
Québec (Québec) G1R 2G4
Phone: (418) 528-7741
Toll Free: 1 (888) 528-7741
Fax: (418) 529-3102

Unionized employees always maintain their rights to grieve under the appropriate collective agreement and, where applicable, employees have the right to contact their respective provincial Privacy Commissioner.