G4S Canada
Human Resources

Privacy Policy

February 2017

Purpose of this Policy

The purpose of this policy generally is to outline how G4S handles the personal information of its customers, employees and other individuals.

In particular, this Policy describes the way that G4S will, subject to applicable legal requirements, adhere to all relevant federal and where applicable, provincial legislative privacy requirements. The Policy follows the ten Canadian Standards Association (CSA) principles identified in the federal Personal Information Protection and Electronic Documents Act (PIPEDA). This Policy describes each principle and the method of implementation. G4S will strive to meet or exceed federal and provincial legislative requirements and will ensure that it remains current with changing technologies and laws.

For the purpose of this Policy, the term "personal information" means any information about an identifiable individual.

Personal information includes, without limitation, an individual's name, home address, home phone number, e-mail address, identity verification information, social insurance number, physical description, age, gender, salary, education, professional designation, personal hobbies and activities, medical history, employment history, credit history, contents of resume, references, interview notes, performance review notes and emergency contact information.

Part 1: Accountability

a. G4S has appointed a staff person (the "Privacy Officer") whose responsibilities will include those of the implementation and monitoring of the G4S Privacy Policy. The Privacy Officer is responsible for G4S compliance with privacy principles. This person will also be responsible for responding to access requests in accordance with this Policy. The Privacy Officer will report to the President and the ultimate responsibility for Privacy issues will rest with the G4S Board of Directors. The Privacy Officer may at his/her discretion enlist assistance from other staff members and/or volunteers within the organization. This will not in any manner mitigate their responsibility for Privacy issues.

b. The Privacy Officer's identity is fully disclosed and publicly accessible to G4S members and the public in general. In Canada, the Privacy Officer and designate alternate for G4S are: SVP HR, reporting to President/CEO, alternate as designated SVP HR

c. The Privacy Officer will ensure that G4S manages all personal information in its possession in accordance with this Policy including that which may be transferred to a third party. Third party organizations who handle information on behalf of G4S shall be contractually obligated to adhere to the standards of G4S.

d. G4S may designate a Privacy Coordinator.

e. G4S will implement internal policies which will facilitate adherence to this Privacy Policy including but not limited to the following:
    - Implementing and maintaining security measures at all levels designed to protect personal information in G4S' possession;
    - Implementing procedures designed to respond to complaints and/or inquiries;
    - Implementing employee training in all facets of information management, including awareness of G4S' Privacy Policy and policies and procedures developed in accordance with the Policy.

For more information:
privacyofficer@ca.g4s.com • www.g4s.ca • 1-888-717-4447

G4S Canada
Human Resources

Privacy Policy

February 2017

Part 2: Identifying Purposes, Types of Information Collected

2.1 Personal Information belonging to G4S' Customers and Customer's Visitors

G4S shall only collect the information reasonably necessary to perform the security services and deliver the security equipment as agreed to with its customers. Access to our privacy policy, procedures and guidelines will be readily available. Similarly, the process by which challenges may be made to G4S' compliance and/or adherence to the legislation in question shall be readily available and transparent. To obtain further information contact G4S Privacy Officer.

G4S collects personal information from its customers and members of the public for the following purposes:

a. to collect, on behalf of its customers; names, dates, addresses, times of access and times of exit of members of the public to premises for which security services are provided by G4S so as to provide a record of such access and egress to its customers;
b. to provide monitoring and surveillance services for and on behalf of its customers to ensure the safety and security of the premises for which its services have been retained;
c. to collect personal information for the purposes of extending credit to its customers and prospective customers and monitoring the credit of its customers in respect of providing its goods and services;
d. to identify products or services of value to current, past and prospective customers and to sell or promote such products and services of G4S, including direct marketing;
e. to comply with legal and regulatory requirements;
f. to assist in providing security services for customers;
g. to assist in crime prevention and the detection, apprehension and prosecution of offenses.

G4S will obtain assurances and representations that the necessary consents have been obtained from its customers before providing and/or implementing the services set forth above.

2.2 Personal Information belonging to G4S Applicants and Employees

Personal information submitted by an applicant to G4S will only be used by G4S to support a responsible and efficient recruitment and selection process. G4S' recruitment purposes are as follows: matching applicant data with G4S current open positions, communicating G4S recruitment and selection procedures, contacting applicants to schedule interviews/tests, sending information to applicants about other relevant vacancies and, where appropriate, confirming background information. Processing includes obtaining, recording, holding, organizing, transferring, adapting, amending, recovering, consulting, using, limiting, disclosing by transmission, disseminating or otherwise making available, aligning, blocking destroying and erasing recruitment data.

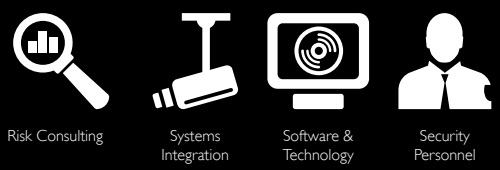
G4S collects personal information of G4S employees in order to properly establish and maintain our employer/employee relationship. Such information will be protected with appropriate safeguards. G4S recognizes the confidential nature of the personal information in its care and its accountability for compliance in protecting this personal information. Accountability extends to all employees of G4S and its directors, officers, managers, employees, representatives and agents including consultants and independent contractors.

During the onboarding process, after an offer of employment an individual may be asked to provide some or all of the following:

- Canadian Social Insurance Number
- A void cheque or direct deposit form from the employee's financial institution

Privacy Policy

February 2017



- Two forms of currently valid Canadian Government issue photo ID; Passport, Birth Certificate, Security Guard License, Permanent Resident Card, Citizenship Card or Certificate, Provincial Photo Identification Card, Card/ Certificate of Indian Status, Age of Majority Card, Work Permit/Work Visa
- Emergency contact information and phone number
- Vehicle Operator's Permit/Driver's License and Abstract (for driving positions)

Personal information will be collected, used and disclosed for purposes pertaining to the individual's employment relationship with the Company, including but not limited to the administration of employee hiring, performance reviews, the administration of employee payroll, processing of employee benefit claims, and for the purpose of complying with all applicable labour and employment legislation.

Purposes for the collection, disclosure and use of personal information:

- to verify past employment references pertaining to an application or offer of employment
- to administer payroll, wages and benefits
- to submit income tax contributions under the Income Tax Act
- to verify an individual's date of birth and other identifying information
- to complete enhanced security screening which may require information obtained from credit bureaus, or credit reporting agencies to comply with the collection and disclosure of personal information for the purpose of legal, regulatory and/or governmental regulations in accordance with the law.

The purposes for collecting personal information will be documented by the Company. Personal information will only be used for the stated purpose or purposes for which it was originally collected. The purposes for which personal information is being collected will be identified orally or in writing to the individual before it is collected.

Part 3: Consent

3.1 G4S will use the personal information for the uses specified above in Section 2 and in Sections 3.2 and 3.3 below.

3.2 In addition to using personal information for the providing of security services, G4S may from time to time wish to use customer names, addresses and contact information for the purposes of providing promotional opportunities, including by providing the information to G4S's marketing and sales departments and other third parties who G4S believes provide services or goods that may be of interest to an individual. G4S and any such third parties may contact an individual with promotional information. G4S will provide an opportunity for the recipient to consent to these opportunities during the registration process. If a recipient consents but later wishes to opt out of this use of information later, they may do so by contacting us as described at Section 3.3 below.

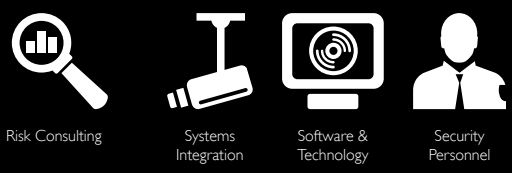
3.3 If at any time an individual wishes to withdraw their consent to the use of their information for any purposes, they may do so by contacting the Privacy Officer for G4S. We will do our best to accommodate this request in a timely fashion without diminishing the services we provide. We will explain the impact of such withdrawal on any services or provisions we provide.

3.4 G4S may collect personal information without consent where reasonable to do so and where it is permitted by law.

G4S Canada
Human Resources

Privacy Policy

February 2017



Part 4: Limiting Collection

All information shall be collected fairly and lawfully within the criteria as set forth in our Privacy Policy.

G4S shall not indiscriminately collect information. The amount and type of information we collect shall be limited to that which is required to fulfill our identified purposes.

Part 5: Limiting Use, Disclosure and Retention

Subject to applicable legislation, G4S shall limit use of personal information it collects to purposes that we have disclosed in Section 2 (Identifying Purposes) and Section 3 (Consent).

G4S shall maintain documents for certain periods of time dependent upon necessity. More specifically:

- G4S may disclose the personal information collected to a government authority that has asserted its lawful authority to obtain the information or where the association has reasonable grounds to believe the information is required for an investigation of an unlawful activity, or to comply with a subpoena or warrant or an order made by the court, person, or body with jurisdiction to compel the production of the information or otherwise as permitted by applicable law.
- G4S may at its discretion release personal information for the purposes of collecting debts which may be owed to G4S and may disclose in this regard the personal information it collects to credit reporting agencies.

Certain documents may be subject to legislated retention periods either federally or provincially and these will be respected at all times by G4S

Part 6: Collection, Storage, Use or Disclosure Outside Canada

In the event that G4S or a service provider to G4S uses collects, stores, uses or discloses personal information outside of Canada, G4S will first provide such notices, policy directions and/or obtain such consents as may be required by applicable legislation.

Part 7: Accuracy

G4S shall strive to ensure to the extent it can that the information entrusted to us is maintained in an accurate manner. We shall try to maintain the interests of the individual and attempt to ensure that decisions are not made for or about an individual based on personal information that is flawed.

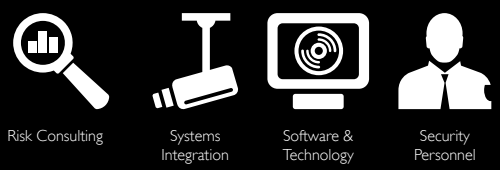
Part 8: Safe Guards

Security safeguards have been implemented to ensure that the personal information collected by G4S is protected from theft as well as unauthorized access, disclosure, copying, use or modification thereof.

For more information:
privacyofficer@ca.g4s.com • www.g4s.ca • 1-888-717-4447

Privacy Policy

February 2017



The level of safeguards employed shall be directly related to the level of sensitivity of the personal information collected. The more sensitive the information, the higher the level of security employed.

Methods of protection and safeguards to be employed shall include but in no way be necessarily limited to locked files, offices and storage areas, security clearances and need to know access as well as technological measures such as passwords and encryption.

Part 9: Openness

G4S will, upon request, disclose the methods by which it handles personal information. The information available includes:

- The name, business address and work telephone number of the Privacy Officer;
- The forms which one may use to access one's information or change your information;
- A description of the type of personal information held by G4S and our general uses thereof.

Part 10: Individual Access

Subject to applicable legislation, upon request by the individual concerned, G4S shall disclose whether or not it actually holds personal information on an individual. We shall disclose the source of this information when requested and provide an account of third parties to whom the information may have been disclosed.

G4S may request sufficient information to confirm the requestor's identity before releasing their personal information.

Subject to applicable legislation, G4S shall endeavour to provide this information within 30 days of receipt of the request for information and only charge nominal fees for the purpose of off-setting expenses incurred in supplying the requested information. This information shall be provided in an understandable format. G4S may under specific circumstances, extend such 30 day period by up to an additional 30 days by contacting the requestor within the first 30 days to explain the reason for the delay, and to advise the individual of their right to complain to the Privacy Commissioner of Canada about the delay. The specific circumstances must be warranted and verifiable for example, if responding to the access request would; (a) interfere to an unreasonable degree with the company's activities, (b) undertake consultations that would make it impracticable to meet the 30-day deadline, (c) if the individual requires the information in an alternate format and it would take a significant amount of time to convert it.

Upon receipt of the information, the requestor may be able to demonstrate that the personal information is incomplete or factually wrong. Inaccurate information that is brought to our attention shall be corrected by G4S as quickly as possible and any pertinent third parties shall be apprised of the corrections in due course.

Part 11 Reporting, Non-Compliance & Complaints

G4S has in place procedures for the resolution of grievances in the administration of its Privacy Policy.
Upon receipt of a complaint G4S shall make available the complaint procedures which will be simple and easy to access.

G4S shall investigate all complaints. If the complaint is deemed justified G4S shall take the appropriate steps to ensure that compliance is achieved and will make changes to its policies to allow for compliance in the future.

G4S Canada
Human Resources

Privacy Policy

February 2017

All complaints shall be addressed in writing to:
G4S Corporate Office,
703 Evans Avenue, Suite 103,
Etobicoke, Ontario, M9C 5E9
privacyofficer@ca.g4s.com
Guidelines for G4S Employees - Safeguarding Privacy/Mobile Devices

Thousands of mobile devices go missing every year in North America. Laptops and 'thumb-drives' get left behind, back-up portable drives and USB keys get misplaced and cell-phones fall out of pockets. Personally identifiable information is any information which may be used to identify an individual. G4S has taken precautions to encrypt and safeguard personal information while working in the G4S office environment. If it is necessary for you to store personal information on a mobile device, you are responsible for safeguarding such information.

- Consider alternatives to storing personal information on a mobile device. Is it possible to access the personal information on a server via a protected remote connection?
- Take only the records that you need to work with.
- Encrypt the data and password-protect the device.
- Do not write down or store passwords and encryption keys on the device.
- Enable the automatic lock feature on your device after five minutes or less of idle time.
- Set your device so Bluetooth is "off" by default, and turn it on only as necessary
- Ensure your mobile device is protected by anti-virus and anti-spyware programs and that they are up-to-date with the latest security patches.
- Use a lockable briefcase or laptop case that does not bear any visible logos of the company. Place an "if found, return by calling (phone number) card inside your briefcase or on the bottom of your laptop with no other identifying information.
- When accessing public wireless networks in hot spots in airports, hotels, coffee shops, public libraries, etc. consider that these networks are open and unsafe. Data transmitted by your device across the open airwaves can easily be picked up and read by another device.
- Do not leave devices containing personal information or other confidential information in your vehicle. When travelling by car, lock your device in the trunk.
- When carrying portable devices, make sure you have each device and all of your belongings when you leave a cab, hotel room, meeting place, airplane or restaurant.
- Secure your device using a cable lock which can be secured to an immovable object.
- When the personal information stored on a mobile device is no longer required ensure that it is deleted completely immediately.
- Ensure that you know exactly what type of personal information is stored on your mobile device in the event that it is lost or stolen.
- If you lose your device or it is stolen, report the loss immediately to the Company and to local police. You may be legally required to notify all individuals potentially put at risk.