Module 8: Legal Authorities

PIPEDA

Overview

Security guards frequently handle the collection, storage, dissemination, protection, and destruction of information. In Canada, several laws, such as the Privacy Act and the Personal Information Protection and Electronic Documents Act (PIPEDA), have been established to safeguard individuals' personal privacy. These laws enforce principles that ensure all entities collecting personal information comply with legal standards.

Key Principles for Security Guards

The following principles have been applied to the general duties of security guards:

1. **Accountability**:
    - Security guards are accountable for the protection of personal information under their control. They should never release private or confidential information without prior authorization from a supervisor or manager. All inquiries related to confidential information should be directed to the appropriate manager.
2. **Identifying Purposes**:
    - Personal information collected during investigations or incidents may pertain to individuals involved in criminal activity, those suspected of involvement, individuals with knowledge of criminal activity, and those who may have information about the identity of suspects.
3. **Consent**:
    - Guards must obtain appropriate consent from individuals for the collection, use, or disclosure of personal information, except when PIPEDA allows for an exception.
4. **Limiting Collection**:
    - The personal information collected by a security guard should be limited to what is necessary for the lawful execution of their duties.
5. **Limiting Use, Disclosure, and Retention**:
    - Information collected by guards cannot be used or disclosed for purposes other than those for which it was collected, except with the individual's consent or as required by law. Personal information should be retained only as long as necessary for the fulfillment of those purposes and should then be destroyed in a legally compliant manner.
6. **Accuracy**:
    - Information collected by security guards should be as accurate, complete, and up-to-date as necessary for the purposes for which it is used.
7. **Safeguards**:

- Guards must ensure that personal information is stored securely in both electronic and hard copy formats. Hard copy files should be stored in locked file cabinets with restricted access.

8. **Openness**:
    - Guards should make readily available to individuals specific information about their companies' and clients' policies and practices relating to the management of personal information.
9. **Individual Access**:
    - Upon request, an individual must be informed about the existence, use, and disclosure of their personal information and given access to it. If such disclosure does not undermine the purposes for which the information was collected, the guard must inform the individual about the personal information held, its use, and any entities or persons who have access to it. Exceptions include:
        - Revealing personal information about another individual.
        - Disclosing commercially confidential information.
        - Information protected under Solicitor/Client privilege.
10. **Challenging Compliance**:
    - An individual must be able to challenge compliance with privacy laws. Guards should know who is accountable for their organization's privacy compliance and how to provide contact information efficiently to individuals raising challenges.

Practical Application of PIPEDA for Security Guards

Accountability: Imagine a scenario where you, as a security guard, encounter a situation requiring the collection of personal information, such as an incident report involving a theft. You are responsible for ensuring that this information is protected and only accessible to authorized personnel. For example, if a colleague asks for details without proper clearance, you must deny the request and refer them to your supervisor.

Identifying Purposes: Suppose you need to gather information from a witness during an investigation. Clearly explain the purpose of collecting their details, emphasizing how it will aid in resolving the incident. This transparency helps build trust and ensures compliance with privacy principles.

Consent: If you need to install a security camera in a specific area, you must inform the residents or employees and obtain their consent. This proactive communication ensures everyone understands the purpose and scope of surveillance, aligning with PIPEDA requirements.

Limiting Collection: When documenting an incident, only record information directly relevant to the case. For instance, if you are investigating a noise complaint, there is no need to document unrelated personal details about the complainant or the offender.

Limiting Use, Disclosure, and Retention: After resolving an incident, securely store the collected information and destroy it once it is no longer needed. For example, if a noise complaint is settled, dispose of any related documents according to your organization's data retention policy.

Accuracy: Ensure that all information recorded during an investigation is accurate and up-to-date. For instance, double-check the details provided by witnesses to avoid discrepancies that could compromise the investigation's integrity.

Safeguards: Use secure methods to store sensitive information. If you are maintaining hard copies of incident reports, ensure they are locked in secure cabinets, accessible only to authorized personnel. For electronic records, use encrypted storage solutions.

Openness: Communicate your organization's privacy policies clearly to individuals when collecting their information. For example, if you are collecting visitor details at a facility, display a notice outlining how their information will be used and protected.

Individual Access: Be prepared to provide individuals with access to their personal information upon request. If a resident requests to see their visitor log entries, ensure you have the process in place to facilitate this access while protecting the privacy of other individuals.

Challenging Compliance: Stay informed about your organization's privacy policies and the designated compliance officer. If an individual raises a concern about how their information is handled, guide them on how to contact the appropriate person to address their challenge effectively.

By adhering to these principles and practices, security guards can ensure they are compliant with PIPEDA and contribute to the protection of personal privacy in their professional duties.