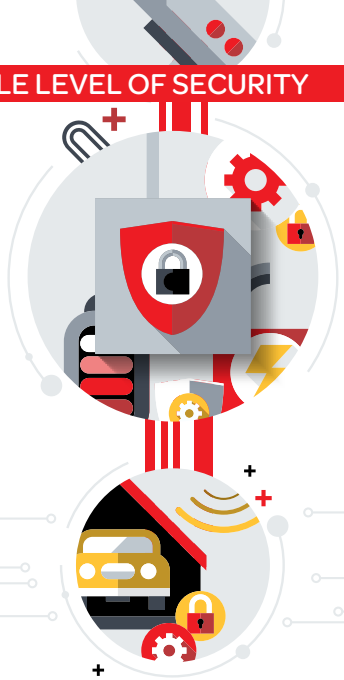
What is a Comparable Level of Protection?

Timothy M. Banks, Dentons Canada LLP



LexisNexis® DENTONS

This is brought to you by Lexis Practice Advisor

As discussed in the practice note, International Data Transfers, an organization transferring personal infor-mation is responsible for ensuring that the recipient organization provides a comparable level of protection for the personal information as would be provided by the transferring organization under applicable Canadian privacy laws. These privacy protections do not have to be equivalent. Instead the organization should review the protections holistically to determine whether the protections are substantially similar.

There are many industry guidelines that can be used to assess the adequacy of the recipient's controls. These include:

- International Standards Organization
  - ISO 27001 (Information technology -- Security techniques -- Information security man-agement systems -- Requirements)
  - ISO 27002 (Information technology -- Security techniques -- Code of practice for infor-mation security controls)
- Payment Card Industry Data Security Standards (PCI DSS)
- Office of the Superintendent of Financial Institutions Cybersecurity Self-Assessment Guidelines (October 28, 2013)
- International Association of CPAs and the Canadian Institute of Chartered Accountants Gener-ally Accepted Privacy Principles (GAPP) and Service Organization Controls Reports (SOC 1, 2 and 3)
- Cloud Security Alliance (CSA) Consensus Assessments Initiative Questionnaire

An organization planning to transfer personal information should choose an appropriate industry guideline to form the basis of an assessment of the controls put in place for the recipient organization. The following checklist may be used as a general guide regarding the types of questions that an organization will need to consider in assessing whether there are comparable safeguards for the personal information being transferred outside of Canada.

Legal Environment	
Does the recipient's jurisdiction have comprehensive legislation governing the protection of personal information?	The organization proposing to transfer personal information should have a clear understanding of the legal norms in the recipient jurisdiction. Although the Canadian law focuses on the adequacy of the organization-to-organization arrangements for the protection of personal information, the legal environment in which the recipient will use or store the information is a relevant consideration in assessing whether there is a comparable level of protection for the personal information. For example, any contractual protections may be meaningless if the organization transferring the personal information will not be able to enforce contractual safeguards or obtain judicial assistance to prevent unauthorized access and use.
Will the recipient have to be registered with a data protection authority or law enforcement agency?	
Are there national security or other similar considerations for Canadians dealing with the recipient's jurisdiction?	
Does the recipient's jurisdiction provide similar protections to the personal information of foreign persons as to its own citizens?	
What is the extent of the powers of law enforcement agencies and governmental organizations to obtain access to data held within that jurisdiction?	
Are law enforcement agencies and governmental organizations able to obtain information without judicial supervision?	
Is it common practice for organizations within the recipient's jurisdiction to cooperate with informal demands for information from law enforcement agencies, governmental organizations and/or other persons?	
Are there any legal impediments to the organization obtaining judicial assistance in the recipient's jurisdiction in the event that the recipient uses or discloses personal information in violation of its agreement with the organization or refuses to return or destroy the personal information in accordance with the organization's direction?	

Administrative Controls	
Does the contract or services agreement provide that the organization transferring the personal information remains in control of the personal information?	The purposes of administrative controls are threefold. First, these controls ensure that there are adequate policies and procedures to safeguard the personal information in the custody of the recipient. Second, these controls are designed to ensure that the organization remains in control of the information even though the recipient has possession of that information. Third, these controls ensure that the organization is able to fulfill its obligations regarding access, correction and breach reporting and notification under applicable Canadian privacy laws.
Is the recipient prohibited from using the personal information for any purpose other than those purposes that are specified and for which the individual has given consent?	
Is the recipient prohibited from using subcontractors or further transferring the personal information without the consent of the organization?	
Does the recipient have appropriate privacy training programs and practices for employees and contractors?	
Does the recipient have adequate controls to limit access to the personal information to those employees and contractors who require access in order to fulfill the purpose for which the information has been collected?	
Is the recipient required to return or destroy the information at the end of the contract or service agreement?	
Does the organization have the right to audit the recipient's processes and procedures? Alternatively, does the recipient publish or make available third party assurance audits of the recipient's processes?	
Is the recipient required to provide access to and correction of the personal information at the request of the organization?	
Is the recipient required to promptly notify the organization of unauthorized access, use, modification, disclosure or destruction of personal information?	
Is the recipient required to cooperate in the investigation of any privacy breach, including assisting in breach reporting to privacy commissioners and individual breach notification, where warranted or legally required?	
Is the recipient obligated to provide notice to the organization of any warrant, subpoena or order to disclose personal information, unless prohibited by law?	
Is the recipient obligated to provide notice of any request for information and not respond to any such request (other than a binding warrant, subpoena or order) without the direction and consent of the organization?	

Technological Controls	
Will the personal information be transferred in a secure manner, such as through strong encryption?	Organizations should not rely solely on broad contractual under-takings by the recipient to maintain appropriate technological se-curity controls. Technological security standards may vary signif-icantly between organizations. As noted earlier, there are many industry standards that can be used to assess the adequacy of the organization's technological controls.
Is the recipient required to keep the personal information segregated from its own data and the data of other organizations?	
Does the recipient use strong authentication methods such as strong passwords, challenge questions, and digital certificates? Is there a documented process for revoking or suspending user IDs and passwords when an employee or contractor leaves the recipient organization?	
Are the authentication methods adequate given the level of sensitivity of the personal information?	
Are there technical controls to prevent the unauthorized copying of the personal information, such as onto unencrypted flash drives?	
Is access to the personal information logged and audited to detect unauthorized activities, including unauthorized copying of data?	
Does the recipient have controls in place to ensure appropriate protection from intrusion, including properly configured firewalls, proxy servers and routers, updated operating systems, anti-virus protection and other similar controls?	
Does the recipient regularly conduct penetration tests and other procedures designed to identify vulnerabilities to intrusion?	
Does the recipient have a disaster recovery plan? Is the disaster recovery plan adequate given the importance of the personal information?	
Will the organization be able to extract the personal information at the end of the contract or service agreement in a useable form?	

Physical Controls	
Does the recipient have perimeter security to prevent unauthorized access to the premises in which the personal information will be stored or used?	Physical controls should not be overlooked. Many privacy breaches occur because of inadequate control over physical assets.
Are all persons who enter the premises logged and required to present identification?	
Does the recipient use closed-circuit video surveillance in areas that house servers and other sensitive areas?	
Is access to sensitive areas controlled by electronic access control?	
Is there a clear physical demarcation of public areas from private areas in which personal information will be used or stored? Is access beyond the public area controlled through electronic access control, name badges or other methods?	
Do the premises have 24-hour security guards?	
Are there any other tenants in the premises? Do they have access to areas in which personal information will be held?	
Do the access controls govern all persons, including contractors? Is there a documented process to revoke access when an employee or contractor leaves the recipient organization?	
Does the recipient restrict the use of personal devices in the work environment to protect against unauthorized copying of data? If not, are there other measures that the recipient takes to prevent unauthorized copying of data?	

LexisNexis®

LexisNexis and the Knowledge Burst logo are registered trademarks of RELX Group plc, used under licence. Other products or services may be trademarks or registered trademarks of their respective companies. © 2015 LexisNexis Canada Inc. All rights reserved.
WebinarCPM-CLS-Whitepaper-09/15