mcmillan

INTERNATIONAL DATA TRANSFERS TO AND FROM CANADA

Posted on September 20, 2016

Categories: Insights, Publications

International Data Transfers to and from Canada in the Era of the Trans-Pacific Partnership and the General Data Protection Regulation: Implementation of Robust Safeguards Measures Protecting Personal Information should be Canadian Businesses' Top Priority

To view the International Data Transfers to and from Canada video click here.

Canada's regime of privacy and data protection is complex. At the centre of this regime lies the *Personal Information Protection and Electronic Documents Act* (PIPEDA)[1], enacted at the Federal level at least partially in response to the European Union's Data Protection Directive (DPD)[2] of 1995. Certain provinces, including Québec, Alberta and British Columbia have adopted substantially similar legislation to *PIPEDA*, which then covers the protection of personal information in those provinces. Both sets of legislation provide comprehensive privacy frameworks, applicable across industries, regulating the collection, use and disclosure of personal information.

For any Canadian company doing business outside of Canada, as is commonplace in the current economic and online environment, it is important to understand not only domestic privacy laws, but also the foreign laws which may affect its partners, customers and suppliers.

EU Data Protection

Across the Atlantic Ocean, the DPD regulates the processing of personal information within EU member states. These member states are required to pass legislation that restricts the transfer of personal information to non-EU countries unless they provide an "adequate level of protection" of personal information, or to entities that have implemented safeguard measures which protect privacy to the same such level (such as through the use of model clauses or Binding Corporate Rules).

PIPEDA (including its provision for recognizing substantially similar provincial legislation) meets this "adequate level" standard, as determined by the EU Commission more than 15 years ago. As such, since 2001, data transfers containing personal information of EU data subjects from EU states to Canada are deemed acceptable and, as a matter of principle, do not require further approval from the European Data Protection Authorities. In more recent years, however, following continued revelations of the ease with which US

surveillance practices may capture data coming from Canada, concerns have arisen with respect to whether the EU Commission's adequacy decision may be in jeopardy.

The Fall of US Safe Harbour

The US enjoyed a similar status to Canada as a jurisdiction providing adequate protection, following Commission Decision 2000/520[3], which held that transfers of personal information of European data subjects from the EU to the US were acceptable where the recipient organisation complied with the EU-US Safe Harbour Principles[4]. However, the Safe Harbour Principles were invalidated following the *Schrems* Case[5], handed down on October 6, 2015 by the European Union Court of Justice, essentially gutting the adequacy determination. Organizations that formerly relied upon the Safe Harbour Principles were left at a loss when suddenly this regime was deemed ineffective and data transfers from the EU to the US were no longer technically sanctioned by the former EU adequacy decision.

Although a new framework, the "US-EU Privacy Shield" was agreed upon between the US and the European Commission in February 2016, Article 29 Working Party, the pan-European data regulator group, criticised the Privacy Shield over its lack of surveillance protection from the US government for EU citizens' data. As a result and in the context of accrued threats to data security, the European approach and data localization requirements are becoming an emerging policy choice for countries concerned with weak privacy protections once personal data is transferred abroad.

The New European Regime

The new General Data Protection Regulation (GDPR), adopted by the European Parliament on April 14 2016, will replace the old DPD. Once the GDPR is formally printed in the Official Journal of the European Union, it will apply directly to each Member State and will harmonize personal data protection across EU nations. While many companies have previously adopted privacy processes and procedures consistent with the DPD, the GDPR contains a number of new protections for EU data subjects and contains significant fines and penalties for non-compliant entities, which may require that companies further adjust.

The GDPR permits personal data transfers to a third country or international organization subject to compliance with a set of conditions. Similar to the framework set out in the DPD, the GDPR allows for data transfers to countries whose legal regime is found by the European Commission to provide an "**adequate**" level of personal data protection. Even without an adequacy decision, transfers are also permitted outside non-EU States under certain circumstances, such as by use of standard contractual clauses or binding corporate rules.

Under the DPD, only persons in approved third countries could receive personal information of EU data subjects, with decisions being made on a country-by-country basis. The GDPR, however, expands the scope of

these adequacy decisions, and allows transfers not only to approved third countries, but also to approved territories or specified sectors within a third country, or even to an international organization. Once the European Commission confers (or retracts) any such adequacy designation, the decision binds all EU Member States.

The TPP ban on creating data transfer restrictions

On the other side of the globe, twelve countries surrounding the Pacific Ocean signed the Trans-Pacific Partnership Agreement (TPP) on February 4, 2016: the United States, Japan, Malaysia, Vietnam, Singapore, Brunei, Australia, New Zealand, Canada, Mexico, Chile and Peru. China is interestingly not a signatory.

The TPP obligates the parties to the Agreement to "adopt or maintain a legal framework that provides for the protection of the personal information of the users of electronic commerce" and, in so doing, "to take into account principles and guidelines of relevant international bodies." A footnote in the directive clarifies that this obligation is met in a variety of ways, including "by adopting or maintaining measures such as comprehensive privacy, personal information or personal data protection laws, sector specific laws covering privacy, or laws that provide for the enforcement of voluntary undertakings by enterprises relating to privacy."

The main purpose of the TPP is to facilitate global trade. From a privacy perspective, the TPP allows cross-border data flows and **prohibits requirements related to data localization**. Each TPP member country is required to "allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business." The inference is that data flow for any commercial purpose would suffice, meaning that personal data ought to flow freely between corporate entities of TPP members, irrespective of jurisdiction.

In the absence of a "legitimate public policy objective," countries **are obligated** to allow this cross-border data transfer conducted in the course of business. In particular, the TPP prohibits nonfinancial laws that require data localization (that is, mandating that companies' computer servers are resident in a country).

Conflicting Forces: GDPR vs. TPP

By establishing a ban on creating data transfer restrictions between signatory countries, the TPP has created a potential conflict with the DPD and the GDPR (which restricts data transfers to only those countries, territories or sectors with laws that meet the "adequacy" standard for protection). There is therefore a risk that, in light of its TPP obligations, the 2001 adequacy decision with respect to Canada could be revoked by the European Commission.

For Canadian companies working with organizations or other bodies located in Europe, it will be important to work proactively to establish rigorous safeguard measures that meet the GDPR requirements (such as

standard data protection contractual clauses or Binding Corporate Rules). In the event that the adequacy decision for Canada is actually revoked, companies with this alternate protection in place will continue to be "safe" recipients of personal information of EU data subjects.

by Michael E. Reid, Darcy Ammerman and Elisa Henry

1.*Personal Information Protection and Electronic Documents Act*, SC 2000, c 5.
2. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995 L 281,p. 31.
3. 2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, OJ 2000 L 215, p.7.
4. Safe Harbor Privacy Principles. issued by the U.S. Department of Commerce, July 21, 2000.
5. *Maximilian Schrems v. Data Protection Commissioner,* Case C-362/14.

A Cautionary Note

The foregoing provides only an overview and does not constitute legal advice. Readers are cautioned against making any decisions based on this material alone. Rather, specific legal advice should be obtained.