AIRD BERLIS

SPOTLIGHT
MEDIA, SPORTS AND COMMUNICATIONS LAW BLOG

Feb 06, 2019

GDPR - Impact on Canadian Business Obligations, Liability and Contract Terms

By Paige Backman

The European Union's General Data Protection Regulation (GDPR) came into effect nearly nine months ago on May 25, 2018. The GDPR clearly applies to those located in the EU, but its application is worldwide in that it expressly imposes obligations, liability and contractual terms on businesses operating outside the EU (including Canada).

The GDPR applies to and imposes obligations and liabilities on both data controllers and data processors that process personal data on EU-based individuals regardless of whether the processing takes place in the EU, where the processing activities relate to the offering of goods or services to individuals in the EU (payment not required) or where there is monitoring of the individual's behaviour where the behaviour being monitored is in the EU. Data controllers determine the purposes and means of the processing of personal data. A data processor processes personal data on behalf of a data controller.

This will impact a significant number of service providers and cloud providers in Canada. Canadian businesses that are processing the data of EU citizens may also have to appoint a representative in the EU.

Breaching the GDPR can result in fines of up to 4% of annual global turnover or €20 Million (whichever is greater). Fines are to be administered by individual member state supervisory authorities and there are criteria such as the nature of the infringements, intentions of the entity in question, efforts to mitigate damages, preventative measures, history of the entity and cooperation. The fines will be tiered in their application with this maximum fine typically imposed in the most serious of infringements.

Contracts with Canadian businesses who process data on EU- based individuals must include provisions complying with Section 28 of the GDPR, such as: processing data solely on the instruction of the data controller; ensuring obligations of confidentiality are imposed on persons who are authorized to processes the data; assisting the data controller with the data subjects' rights request; notifying the data controller of data breaches; assisting the data controller with privacy impact assessments; ensuring any sub-contractor relationships are subject to the same flow-down obligations; and deleting or returning all personal data processed on the controller's behalf at the end of the processing obligations.

Aside from contractual obligations, GDPR imposes organizational obligations on Canadian businesses that are subject to the GDPR, such as: ensuring appropriate technical and organizational security measures; data mapping so organizations know exactly what personal data is where and used for what purposes as well as for purposes of deleting same to comply with the "right to be forgotten"; policies, procedures (and training); appointment of a Data Protection Officer or EU representative; undergoing privacy audits and privacy impact assessments; and privacy by design approaches to products and services.

Many of the GDPR requirements are similar to those under existing Canadian privacy laws (consent, security, contractual terms with subcontractors, etc.). Further, as noted in prior posts on the Spotlight, the Office of the Privacy Commissioner of Canada has interpreted Canada's PIPEDA in a way that further aligns with GDPR (such as interpreting PIPEDA in a way that supports the highly-debated right to be forgotten). Regardless of whether the interpretations can be supported by the language of the legislation, this movement is seen as necessary so that Canada maintains its status of offering equivalent protection to the GDPR so as not to impede the data processing industry between the jurisdictions.

However, the GDPR is more prescriptive in its obligations, whereas Canada's privacy laws are based more on principles and are open for more interpretation. Of course, and here's what makes businesses

stand up and take action, the financial penalties for non-compliance with the GDPR are significantly more severe than under Canada's privacy laws. If Canadian companies think that they will practically be able to avoid GDPR's reach, note that supervisory authorities have already enforced GDPR obligations against non-EU-based entities, including AggregateIQ, a Vancouver, Canada-based business who used personal data to place ads on social media that targeted Brexit voters.

If you need assistance with complying with your privacy, data security or data breach needs, please do not hesitate to contact Paige Backman at pbackman@airdberlis.com or 416.865.7700.

Author

Paige Backman
Partner
T 416.865.7700
pbackman@airdberlis.com