McCarthy Tétrault *Advance*™
Building Capabilities for Growth

The Application of GDPR to Canadian businesses: Are you ready?

Charles Morgan, Partner
Direct Line: (514) 397-4230
E-Mail: cmorgan@mccarthy.ca

May 10, 2018

Presentation

- Scope of Application
  - EU Establishments
  - Non-EU Established Businesses
- Major Changes
  - Consent
  - Data Protection by Design
  - Data Portability
  - Right to be Forgotten
  - Data Breach Reporting
  - Sanctions
- Implications for Canadian Businesses
  - Expanded Scope of Application
  - Accountability and Data Mapping
  - Refreshing Data Protection Policy, Consents and Procedures
  - Modifications to CRM functionality
  - Data Transfer Agreements

Context

- One of the most wide-ranging pieces of legislation passed by EU in years
- Result of 4 years of debate over draft GDPR published in Jan 2012
- Adopted April 2016; takes effect May 25 2018
- An EU data protection regime change:
  - That applies directly to many Canadian companies
  - That may provide « advance notice » of changes to come in our own data protection regime

Where goes the EU data protection regime; thither goes Canada's privacy regime also?

Part 1: Territorial Scope of Application

- EU “established” controllers or processors
  - An “establishment” in the EU where personal data are processed
  - Where it exercises “any real and effective activity – even a minimal one”
- Non-EU “established” organizations that target or monitor EU data subjects
  - Offering of goods or services (payment not required)
  - Monitoring of behaviour (e.g. online behaviour)

Are you sure the GDPR does not apply to you?

Application to EU-based establishments

- The *Weltimmo* court considered whether Weltimmo, a Slovakian company operating a website targeting the Hungarian market, had an establishment in Hungary. Weltimmo processed the data of Hungarian users who advertised properties on the website.
- The court stated that the existence of an establishment only requires **a real and effective activity, even a minimal one**, exercised through stable arrangements.
- The CJEU took into consideration several factors, including:
  - The permanent local presence of the representative in Hungary.
  - The use of a Hungarian mailbox and bank account for business purposes.
  - Representation of the company in various court and administrative proceedings through a local representative.
  - A website in Hungarian language targeted at Hungary.

Application to EU Establishments

- In *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* (Case C-131/12), the CJEU examined whether Google Inc., a US based search engine processing Spanish data subjects' personal data in the US, had an establishment in Spain based on its Spanish subsidiary's activities.
- The CJEU ruled that Spanish data protection law applied to Google Inc.'s personal data processing because that **processing was "inextricably linked to" and therefore carried out "in the context of the activities of"** Google Spain.
- Non-EU based data controllers and data processors that:
  - process personal data outside of the EU;
  - have an establishment in the EU through, for example, an affiliate, subsidiary, or branch; and
  - an inextricable link exists between the processing activities and the EU establishment

Application to Non-EU Established Businesses

- Non-EU organizations **processing EU data subjects' personal data in connection with offering goods and services in the EU** are subject to GDPR
- The following GDPR factors will help organizations make this assessment:
  - Whether the business offers goods or services in an EU language or currency.
  - Whether the business allows EU data subjects to place orders in the local language.
  - Whether the business refers to EU customers when marketing its goods and services
- Other evidence may show intent to target EU data subjects including, for example, a business plan describing efforts to obtain EU customers.

Application to Non-EU Established Businesses

- The GDPR applies to non-EU established data controllers and data processors that process EU data subjects' personal data in connection with monitoring their activities in the EU
- GDPR states that monitoring takes place when organizations track individuals on the internet and use personal data to:
  - Profile a natural person to make decisions concerning her or him.
  - Analyze or predict personal preferences, behaviors, and attitudes.
- Profiling under the GDPR includes any form of automated processing of personal data about a person to analyze or predict the individual's:
  - Performance at work.
  - Economic situation.
  - Health.
  - Personal preferences.
  - Interests.
  - Reliability or behavior.
  - Location or movements.

Part 2: What's New?

Transparency and Consent

- Presumption that consent is not valid unless separate consents obtained for separate processing activities Data subject must have right to withdraw consent
- Consent requests presented in concise, transparent, easily accessible manner
- Children under 13 can never, themselves, consent to processing of their data
- “Legitimate interest” must meet the “reasonable expectations of the data subject based on his or her relationship with the data controller”.

No « omnibus » consents!
Update your Data Protection Policy

Information Obligations

When the data controller collects personal data directly from a data subject, it must first inform the data subject about:

¬The data controller's identity and contact details, and if applicable, its EU representative's identity and contact details.

¬Contact details for the data controller's data protection officer, if applicable.

¬The purposes for which the data controller processes any personal data collected.

¬The legal basis for the processing.

¬Identification of the data controller's legitimate interests when they serve as the legal basis for data processing.

¬The recipients or categories of recipients of the personal data, if any.

¬Whether the data controller intends to transfer personal data outside of the jurisdiction and the data transfer mechanism it uses to legalize the transfer.

¬How long the data controller stores the personal data or the criteria the data controller uses to determine retention periods.

¬Whether the data subject must provide the personal data by statute, contract, or for another reason, and the consequences of not providing the personal data.

¬Whether the data controller uses automated decision-making, including profiling, the auto-decision logic used, and the consequences of this processing for the data subject.

Data Protection by Design and by Default

- Where « high risk » processing undertaken, must implement « privacy impact assessment »
- Use of pseudonymisation: process data in a manner that separates personal data from identifiable data subject
- High duty of care in selecting personal data processing service providers
  - Approved data processing standard clauses may be published
- Staff training

Newly coined term: pseudonymisation!

Data Portability

- Data subjects can request that their personal data be ported to them or to a new provider in a machine-readable format
- Request must be met within one month

Data subjects have greater control over their data

« Right to be Forgotten »

A data subject has the right to request erasure of their personal data if one of the following applies:

- The personal data is no longer necessary for the purpose the data controller collected it for.
- The data subject withdrew its consent to the data controller's processing activities and no other legal justification for processing applies.
- The data subject objects to processing for direct marketing purposes.

If the data controller made the personal data public, the data controller must also take reasonable steps, including technical measures, to inform other data controllers that are processing the personal data about the data subject's erasure request.

Data Breach Reporting

- Data processors must report personal data breaches to data controllers
- Data controllers must report to supervisory authority and, in some cases, to data subjects
- Must maintain internal breach register

Sound familiar?

Sanctions

- Breaches of basic requirements (e.g. Consent)
  - Article 83 of the GDPR can amount to 4% of the total ***worldwide*** annual turnover of a company or €20,000,000, whichever is higher
- Breaches of data breach requirements:
  - Article 83 of the GDPR can amount to 2% of the total worldwide annual turnover of a company or €10,000,000, whichever is higher

Ouch!

Part III: Implications for Canadian Businesses

- Expanded Scope of Application
- Data Mapping
- Refreshing Data Protection Policy, Consents and Procedures
- Modifications to CRM functionality
- Data Transfer Agreements
- Data Protection Impact Assessments

Be Prepared for the EU GDPR

- Privacy by Design and Privacy by Default
- Data Portability
- Right to be forgotten
- Right to access – copy of personal information file, free of charge, in an electronic format
- Advertising based on PI – opt-in
- Breach notification within 72 hours of becoming aware of the breach

VANCOUVER

Suite 2400, 745 Thurlow Street
Vancouver BC V6E 0C5
Tel: 604-643-7100
Fax: 604-643-7900
Toll-Free: 1-877-244-7711

CALGARY

Suite 4000, 421 7th Avenue SW
Calgary AB T2P 4K9
Tel: 403-260-3500
Fax: 403-260-3501
Toll-Free: 1-877-244-7711

TORONTO

Box 48, Suite 5300
Toronto Dominion Bank Tower
Toronto ON M5K 1E6
Tel: 416-362-1812
Fax: 416-868-0673
Toll-Free: 1-877-244-7711

MONTRÉAL

Suite 2500
1000 De La Gauchetière Street West
Montréal QC H3B 0A2
Tel: 514-397-4100
Fax: 514-875-6246
Toll-Free: 1-877-244-7711

QUÉBEC

500 Grande Allée Est, 9e étage
Québec QC G1R 2J7
Tel: 418-521-3000
Fax: 418-521-3099
Toll-Free: 1-877-244-7711

UNITED KINGDOM & EUROPE

125 Old Broad Street, 26th Floor
London EC2N 1AR
UNITED KINGDOM
Tel: +44 (0)20 7489 5700
Fax: +44 (0)20 7489 5777

mccarthy tétrault