THE GDPR – KEY POINTS FOR CANADIAN BUSINESSES

Posted on August 5, 2016

Categories: Insights, Publications

Background

In 1995 the European Union ("EU") adopted the Data Protection Directive (the "Directive") which regulates the processing of personal data within the EU. The Directive provides guidelines for the development of privacy law in Member States. Since the Directive is not itself a binding law on companies and individuals, each Member State was required to implement its own law. This has created a patchwork of privacy laws across the EU that adhere to the basic principles of the Directive.

On April 14, 2016, the European Parliament approved and adopted the General Data Protection Regulation (GDPR) to bring a single cohesive system of privacy regulation to the EU. The GDPR was published in the EU Official Journal on May 4, 2016 and will come into force on May 25, 2018. The EU intends for this single law to strengthen the protection of individual privacy rights and simplify business rules for companies operating in the EU market.

Territorial Reach

Currently, under the Directive, a Member State's laws apply to companies in three situations:

1. The company is processing personal data on a site in the territory of the Member State;
2. The company is established in a place where the Member State's national law applies; or
3. The company processes data using equipment located in the territory of the Member State, unless it is only used for transit through the territory.

When the GDPR comes into force, it will apply to companies that have an establishment in the EU or that engage in data processing activities that relate to:

1. Offering goods or services to EU residents; or
2. Monitoring the behaviour of EU residents within the EU, which may include tracking internet activity for behavioural advertising purposes.

Therefore the GDPR has a wider reach than the Directive and has the potential to impact companies that do not have any operations in the EU. Below is an overview of some of the key differences between the Directive

and the GDPR, as well as steps Canadian organizations can take now to begin preparing for the GDPR.

Consent

Under the Directive, consent has to be unambiguously given by the individual. It can be implied in limited circumstances, for instance if the data processing is necessary to perform a contract with the individual. Consent can also be inferred from the actions or inactions of the individual, which allows companies to rely upon "opt-out" consent provided that it is clear that the individual had to opt out. Finally, explicit consent is needed for sensitive personal data, unless the processing of that information is necessary for a specified purpose (e.g., for employment law related matters).

Under the GDPR there will be several changes to the EU's approach to consent:

1. "Opt-out" consent does not appear to be permitted. Consent must be freely given, specific, informed, unambiguous, and given through some clear action;
2. Explicit consent will be required for sensitive data and there must be an option for individuals to withdraw or refuse such consent;
3. All individuals will have the right to object to direct marketing and profiling related to direct marketing, and they must be informed of this right;
4. There will be a presumption against consent if there is a clear imbalance of power, which would tend to be the case between companies and consumers;
5. Specific consent will be required for each new data processing operation, unless the subsequent operations are sufficiently similar to ones already consented to;
6. Companies will only be allowed to offer services conditional on consent if the data processing is integral to providing the service;
7. Any child under 16 will require parental consent, unless a Member State opts to reduce the age to 13; and
8. Companies must make the right to withdraw consent as easy as giving consent, and must inform users of this right.

Accountability

The Directive provides some limited restrictions on the collection and retention of personal data, including a requirement to implement certain security measures based on the nature of the data and the associated risks. The GDPR, however, incorporates the "privacy by design" principles that are recognized in Canada. The GDPR also contains additional accountability requirements, including but not limited to:

1. Stricter data protection policies and procedures;
2. Enhanced record keeping obligations;

3. Requirements for data protection impact assessment for high risk activities; and
4. Requirements for stronger security measures matching the risk of data breaches and potential harm to individuals.

Data Breach Notification

The EU does not currently impose a legal obligation on companies to inform individuals of a data breach. When the GDPR comes into force, companies will have to notify individuals without delay that there has been a breach of their personal data. Where possible this notification will need to be provided within 72 hours, unless the breach is unlikely to impact the rights and freedoms of individuals. The GDPR also includes a duty for data processing companies (the "Processors") to report breaches to the company that collected and controls the data they process (the "Controller").

Data Processors

The current EU law places most obligations for processing on the Controllers. Controllers are required to select a Processor that will implement sufficient protection and the data processing must be governed by a contract pursuant to which the Processor must only act on the instructions of the Controller and must agree to abide by the Member State's law where the Processor is established.

The GDPR alters the current scheme and will spread obligations more evenly between Controllers and Processors. Controllers still bear the primary burden for protection of personal data and must select a Processor that will implement sufficient protections. The Controller will also be obligated to carry out a "Privacy Impact Assessment" for high risk processing and must keep records of processing activities. However, Processors will now be subject to direct regulation, including the obligation to process data only as instructed by the Controller, use appropriate safeguards, return or delete data once processing is complete, and notify the Controller of any data breaches. Processors also cannot subcontract any obligations without the Controller's permission. The GDPR contains detailed requirements for contracts that govern the Controller-Processor relationship.

International Transfers

Currently, the Directive restricts transferring personal data to a country outside the EU unless the recipient jurisdiction offers "adequate" protection for such information, subject to certain exceptions at the Member State's discretion (e.g., Member States may allow a transfer to a country that does not ensure adequate protections if the Controller shows they have sufficient safeguards in place).

The GDPR contains stricter restrictions upon transferring personal data to countries that do not have adequate protections in place. However, transfers will still be permitted to those countries if the Controller has approved

"binding corporate rules" or has entered into an agreement that contains the required "standard contractual clauses". The GDPR also includes two new allowable mechanisms for international transfers of personal data:

1. Binding and enforceable codes of conduct; and
2. Certification by a body that meets certain accreditation requirements and complies with certain responsibilities under the GDPR.

Data Protection Officers

Under the Directive, companies are not obligated to employ a data protection officer ("DPO"), although some Member States have such a requirement under their local laws. The changes under the GDPR will require companies to appoint a DPO in certain circumstances, including if the company's processing of personal data requires regular and systematic monitoring of data subjects on a large scale or the core activities of the company consist of processing special categories of data on a large scale.

DPOs are given certain rights under the GDPR including:

1. A right to not be dismissed or penalized for performing their responsibilities;
2. A right of access to data processing personnel and operations;
3. A right to significant independence; and
4. A right to have a direct reporting line to the highest level of management.

Right to be Forgotten

The right to be forgotten has developed through EU case law, however, it will be enshrined in legislation when the GDPR comes into force. Subject to certain conditions, Controllers will be obligated to erase personal data without undue delay in certain circumstances, for instance: if the data is no longer needed, if an individual objects to processing, or if the processing was unlawful. Controllers who have received a request to delete certain data must also take reasonable steps to inform other Controllers, who have had access to the data, of that individual's request.

Sanctions

Under the Directive there is no unified set of sanctions. Member States are responsible for their own suitable sanctions and must provide for a judicial remedy for a breach of privacy rights.

The GDPR contains significant sanctions for companies found to have violated legal rights and obligations related to data processing. There will be two tiers of possible sanctions:

1.The upper tier, where serious infringements will attract a penalty of the greater of:

i. 20,000,000 Euros, or

ii. 4% of annual worldwide turnover of the corporate group; and

2.The second tier, where lesser infringements will attract a penalty of the greater of:

i. 10,000,000 Euros, or

ii. 2% of annual worldwide turnover of the corporate group.

The GDPR will also allow public interest organizations to bring class actions for data breaches on behalf of individuals who have had their rights violated.

Steps to Consider

Many of the restrictions and requirements set out in the GDPR are consistent with requirements under the *Personal Information Protection and Electronic Documents Act* ("PIPEDA"), and therefore, Canadian organizations that already comply with PIPEDA or substantially similar provincial legislation may already have many appropriate privacy policies and practices in place.

However, given the seriousness of the potential sanctions under the GDPR, affected organizations would be well advised to begin taking steps now to consider and address the specific requirements of the GDPR where they differ from PIPEDA. For example, organizations may need to:

1. Review consent forms for EU residents to determine if amendments are necessary to comply with the GDPR;
2. Review contracts with Data Processors, as well as the organization's selection process for Data Processors, to ensure compliance with the specific GDPR requirements;
3. Ensure that the Company's Chief Privacy Officer's ("CPO") qualifications, duties and placement within the organization are consistent with GDPR requirements (or hire/appoint a new DPO or CPO, with the required expertise, if necessary);
4. Thoroughly review privacy and data protection policies and practices that apply to the handling of personal data of EU residents, to ensure compliance with the GDPR;
5. Review the organization's privacy compliance infrastructure to determine if adjustments need to be made in light of the GDPR accountability requirements; and
6. Consult with legal counsel to understand the organization's legal obligations and ensure that appropriate steps are taken to meet these obligations before the GDPR comes into force.

Organizations that begin taking steps now, to comply with the GDPR, will be better positioned to meet their legal obligations when the legislation comes into force, and thereby avoid potentially significant penalties.

by Lyndsay Wasser and Bob Bell, Student-at-Law

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.