The General Data Protection Regulation (GDPR) – Implications for Canadian Organizations

By Bill Hearn, Fogler, Rubinoff LLP , Paul Lewis, Nymity
and Scott Pink, O'Melveny & Myers LLP

Lexpert's 9th Annual Information Privacy and Data Protection Conference
November 30, 2017, Toronto

fogler rubinoff

NYMITY innovating compliance

O'Melveny

OUTLINE

- What is the GDPR and how does it change the privacy landscape?
- What is the eP Reg and why does it matter?
- What should Canadian organizations be doing about the GDPR?
- What are the implications of the GDPR for PIPEDA's "adequacy" status on trans-border data transfers? And what are the alternatives and derogations?
- What is the status of the EU-US privacy shield?
- Key takeaways

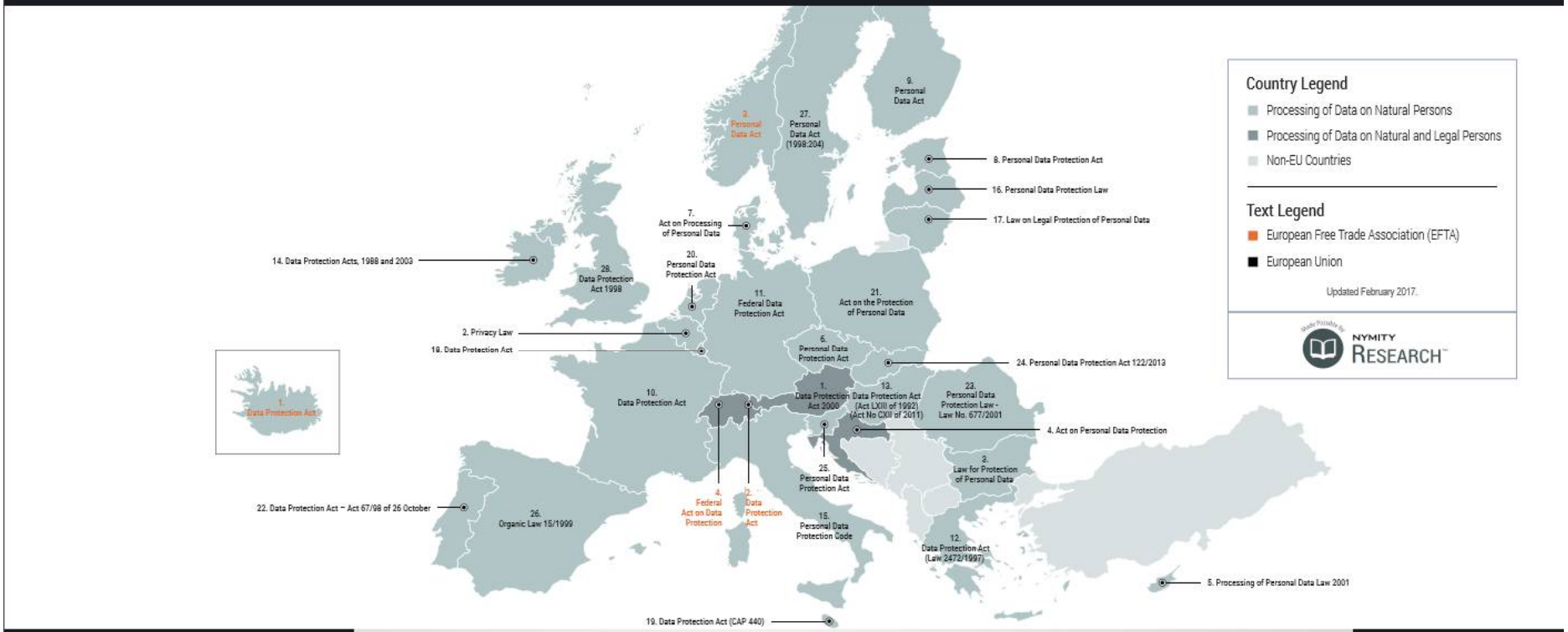
fogler rubinoff NYMITY innovating compliance O'Melveny

THE GDPR & HOW IT CHANGES PRIVACY LANDSCAPE

NYMITY
innovating compliance

AS-IS…

Primary Data Protection Laws in the European Union and the EFTA



NYMITY
innovating compliance

EU Members

1. **AUSTRIA:** Federal Act Concerning the Protection of Personal Data (Datenschutzgesetz 2000 – DSG 2000)
2. **BELGIUM:** Law of December 8 1992 on the protection of privacy in relation to the processing of personal data
3. **BULGARIA:** Law for Protection of Personal Data
4. **CROATIA:** Act on Personal Data Protection
5. **CYPRUS:** The Processing of Personal Data (Protection of Individuals) Law 138 (I) 2001
13. **HUNGARY:** Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information
14. **IRELAND:** Data Protections Acts, 1998 and 2003
15. **ITALY:** Personal Data Protection Code – Legislative decree n° 196 of 30 June 2003
16. **LATVIA:** Personal Data Protection Law
17. **LITHUANIA:** Law on Legal Protection of Personal Data
22. **PORTUGAL:** Act 67/98 of 26 October – Act on the Protection of Personal Data (transposing into the Portuguese legal system 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)
23. **ROMANIA:** Law No. 677/2001 on the Protection of Individuals with Regard to the Processing of

EFTA

1. **ICELAND:** Act on the Protection of Privacy as regards the Processing of Personal Data, No. 77/2000 of May 10, 2000
2. **LIECHTENSTEIN:** Data Protection Act of 14 March 2002
3. **NORWAY:** Act of 14 April 2000 No. 31 relating to the processing of personal data (Personal Data Act)
4. **SWITZERLAND:** Federal Act on Data Protection (FADP) of 19 June 1992

Regulation

General Data Protection Regulation (GDPR) Regulation (EU) 2016/679 (Enters into application 25 May 2018)

Directives

1. **General Directive**
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

2. **Directive on Privacy and Electronic Communications**
Directive 2002/58/EC amended by Directive 2009/136/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications

NYMITY
innovating compliance

PURPOSE…

- It is intended to simplify the regulatory environment for international business To enhance the level of data protection for EU data subjects
- EU data subjects will have more control over their personal data
- Extends “reach” – not dependent on geographical processing - applying to controllers and processors, both inside and outside the EU, whose processing activities relate to the offering of goods or services to EU data subjects.
- To modernize the regulation in line with existing and emerging technologies – a lot has happened!
- More options for international transfers
- Data Protection Authorities have the power to impose significant fines on organizations for non-compliance with the rules, scalable to €20 million or 4% of the organization’s global annual turnover per incident, whichever is greater.

NYMITY
innovating compliance

IMPLEMENTATION…

- Unlike the prior 1995 EU Data Protection Directive, the Regulation does not require any further enabling legislation to be passed by specific country governments It will be "automatic" in the 28 EU Member States, and those countries following EU law voluntarily. In practice we will see implementing legislation…

Member State Implementing Laws and Bills

Enacted Laws:
Austria - Amendments Adopted to the Austrian Data Protection Act
Germany - Act to Adapt Data Protection Law to Regulation (EU) 2016/679 and to Implement Directive (EU) 2016/680 (DSAnpUG-EU)
Draft Bills:
Belgium - Bill 2648-001 - On the Creation of the Data Protection Authority
Czech Republic - Data Protection Bill and Bill Amending Other Laws
Hungary - Preliminary Draft of GDPR Implementation Act
Ireland - General Scheme of the Data Protection Bill 2017
Latvia - Personal Data Processing Bill - Ministry of Justice
Lithuania - Bill Amending the Personal Data Protection Act No. I-1374
Luxembourg - Bill No. 784 Implementing and Complementing GDPR and Repealing Law of 2 August 2002
Netherlands - Rules Implementing the GDPR and Repealing the General Directive
Poland - Draft Law on Personal Data Protection
Romania - Draft Law Amending Law No. 102/2005 on Data Protection Authority Powers and Repealing Law. No. 677/2001
Slovenia - Draft Law on the Protection of Personal Data
Slovakia - Law on Personal Data Protection
Spain - Proposed Draft Updating the Organic Law or Protection
United Kingdom - HL Bill 66 - Data Protection Act 2017 - UK Parliament

Non-Member State Implementing Laws and Bills

Draft Bills:
Argentina - Draft Bill to Reform the Personal Data Protection Act
Guernsey - The Data Protection Law Bailiwick of Guernsey Law 2017
Serbia - Model Law on Protection of Personal Data

NYMITY
innovating compliance

GDPR PERSONAL DATA

- Per the GDPR, the definition of “Personal Data” now explicitly includes online identifiers, location data and biometric/genetic data – e.g. call Centre voice authentication
- Includes data in Mobile Devices, IoT etc.

NYMITY
innovating compliance

GDPR HIGHER STANDARDS…

- Higher standards for privacy policies and statements
- Higher standards for obtaining consent
- Easier access to personal data by a data subject
- Enhanced right to request the erasure of their personal data "right to be forgotten"
- Right to transfer personal data to another organization (portability) - How? Ease of transfer implications…
- Right to object to processing now explicitly includes profiling. (catching big data processing, analytics)
- Operationalization of Privacy by Design as default

NYMITY
innovating compliance

ENHANCED OBLIGATIONS FOR PROCESSORS…

- Increased obligations for data processors
- What does this mean for cloud? IaaS, SaaS etc.
- Management of 3rd and 4th party data processors
- Implementation of technical and organizational security measures (TOMs) appropriate to the risks presented
- Provide security and privacy controls and audit
- Assistance with breach response

NYMITY
innovating compliance

GDPR BREACH NOTIFICATION

- Personal Data Breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized access to, personal data transmitted, stored, or otherwise processed
- Much broader than NA concept of breach of information that may lead to fraud or identity theft
- Must notify DPA within 72 hours (justification required if not met) and communicate information regarding the breach to the affected data subjects “without undue delay”
- UNLESS IMPLEMENTED TOMS TO RENDER IT UNREADABLE TO UNAUTHORIZED INDIVIDUALS SUCH AS ENCRYPTION

NYMITY
innovating compliance

GDPR DATA HOLDING/PROCESSING PARADOX

- Do I know what I know?
- Legacy data systems and holdings, unstructured data sets, reports, branch level systems, backups
- OLD: Registration and Purposes of Data Holdings with each DPA
- NEW: Record of Processing
  - On demand – Article 30 Report
  - Sensitive data = DPIA -> Article 35 Report
- Intent and what we are seeing happen…

NYMITY
innovating compliance

GDPR LAWFUL PROCESSING

- With consent
- for contract performance
- to comply with legal obligations under Union or Member State law
- to protect the vital interests of a natural person
- to perform a task in the public interest set out by Union or Member State law
- or for the purposes of legitimate interests pursued by the data controller or a third party.

NYMITY
innovating compliance

ACCOUNTABILITY

- Accountability principle in Article 5(2) of the GDPR requires organisations to demonstrate compliance with the principles of the GDPR. Article 24 sets out how organisations can do this by requiring the implementation of appropriate technical and organisational measures (TOMs) to ensure that organisations can demonstrate that the processing of personal data is performed in accordance with the GDPR.

ACCOUNTABILITY

- Sample Accountability TOMs:
  - Guidelines, policies or assessments around when DPIAs are required
  - Data privacy training
  - Template consent forms
  - Records retention schedule
  - Data quality procedure
  - Validation mechanisms in online forms
  - Information security policy
  - Encryption policy
  - Identity access management with access rights restricted on a “need-to-know” basis
  - Security risk assessment
  - Software tools for data masking

NYMITY
innovating compliance

WHAT IS THE eP REG AND WHY DOES IT MATTER?

fogler rubinoff

eP REG

- On May 25, 2018*, the ePrivacy Regulation (the "**eP Reg**") *may* replace the existing EU ePrivacy Directive (colloquially known as the "EU Cookie Directive")
  - * Many EU lawyers say this proposed "in force" date is not achievable and don't expect the eP Reg to become law until 2020
  - The eP Reg was officially published by the European Commission only on January 10, 2017 and is a law separate from the GDPR
- It complements and is aligned with the GDPR in that
  - a breach can attract the same severe financial penalties – i.e., up to the greater of €20 million or 4% of worldwide turnover
  - it will be enforced by the same supervising authorities – i.e., the national privacy and information regulators of EU Member States

fogler rubinoff

eP REG

- The eP Reg attempts to reinforce trust and security in EU's digital market
- It will establish a new privacy legal framework for electronic communications
- It has a very wide scope and will broadly apply to any organization that provides any form of online communication service, or that utilizes tracking technologies, or that engages in electronic direct marketing

fogler rubinoff

eP REG

- Specifically, the eP Reg will apply to
  - organizations *anywhere in the world* that provide publicly-available "electronic communications services" to users in the EU or that gather data from the devices of users in the EU. It applies even if there is "no charge" for the services
  - traditional ISPs and telcos … but also to so-called "over-the-top" providers, such as VOIP services, text messages and email providers that are not subject to the current ePrivacy Directive
  - all electronic communications data which includes both content (i.e., what was said) and metadata (i.e., who said it, when, where, and other related info about the communication)
  - anyone using cookies or similar tracking technologies
  - IoT and machine-to-machine communications

fogler rubinoff

eP REG

- Among other things, the eP Reg
  - enhances “consent” requirements in line with the GDPR … and end-users must be reminded every 12 months of their right to withdraw consent
  - requires website providers to present users with cookie consent choices
    - some EU legal commentators say this may lead to the end of cookie banners in that clear affirmative action will be required to signify freely given, specific, informed and unambiguous consent to the storage and access of third party tracking cookies
    - consumers will be the ones setting their privacy settings via their browsers or any mobile apps they use
  - keeps exemption for analytics cookies

fogler rubinoff

eP REG

- For direct e-marketing, the eP Reg provides that
  - if B2C, the sender must obtain the opt-in consent of the recipient … but consent will not be required when marketing similar products and services so long as the recipient is given the opportunity to object and opt-out
  - if B2B, each Member State may put in place whatever it deems appropriate to ensure that the legitimate interests of corporate end-users are sufficiently protected from unsolicited e-communications

fogler rubinoff

WHAT SHOULD CANADIAN ORGANIZATIONS BE DOING ABOUT THE GDPR?

fogler rubinoff

GET TO KNOW THE GDPR

- Canadian organizations must first be made aware of the GDPR
- They must then assess to what extent the GDPR applies to their activities and what changes may be required to comply
- The organization's legal and privacy professionals should make sure that key decision makers within the organization know that the EU's privacy law will soon be changing to the GDPR – i.e., **on May 25, 2018**
- If an organization is somehow unaware of the GDPR, the time to act is NOW!
- CASL-compliance fatigue (while understandable) is no excuse for inaction

fogler rubinoff

FIGURE OUT IF GDPR APPLIES

- Many Canadian organizations will be subject to the GDPR because they
  - have an establishment/physical presence in the EU or
  - collect or process personal data of EU residents for offering goods or services (even at no charge) or
  - monitor the behaviour of individuals in the EU or
  - are a third party processor of EU personal data

fogler rubinoff

RESTRICT ACTIVITIES OR COMPLY?

- If the GDPR applies to a Canadian organization's activities, that organization must decide whether
  - to restrict their activities so that they fall outside of the scope of the GDPR
    - e.g., stop providing services to EU residents … or stop processing data from individuals in the EU or
  - to comply with the GDPR

- If the decision is made to comply, then the Canadian organization must determine what GDPR obligations apply to it

fogler rubinoff

TAKE STEPS TOWARDS COMPLIANCE

- The organization should conduct a compliance assessment of current data protection policies and practices in order to identify gaps in relation to the GDPR's requirements
  - If enforcement action is ever taken by the EU in the future, such an assessment may help the organization mount a successful defence or at least mitigate fines

- Following this assessment, the organization can then develop strategies to achieve GDPR compliance in an effective and cost efficient manner
  - e.g., consider whether it is possible for the organization to isolate all of its data that is subject to the GDPR and then implement a compliance plan only in respect of that data (as opposed to a plan across the entire organization)

fogler rubinoff

TAKE STEPS TOWARDS COMPLIANCE

- There are many similarities between PIPEDA and the GDPR
- So, Canadian organizations that are already PIPEDA-compliant have less work to do and should focus on designing and implementing policies and practices regarding those aspects of the GDPR where there is no PIPEDA equivalent – such as ensuring the rights of individuals to
  - data portability (i.e., to port their personal data to another organization)
  - erasure (i.e., right to be forgotten)
  - object to marketing and to decisions taken by automated processes
  - breach notification
    - e.g., "without undue delay and, where feasible, not later than 72 hours after having become aware of it"; if the notification is not made within 72 hours, the data controller must provide a "reasoned justification" for the delay

fogler rubinoff

TAKE STEPS TOWARDS COMPLIANCE

- There are several steps for the organization to consider including reviewing and revising where required by the GDPR
  - consent forms for EU residents
  - the selection process for, and contracts with, data processors
  - the qualifications, placement and duties of the organization's chief privacy/data protection officer
    - DPOs must be independent and not instructed how to do their job
  - privacy and data protection policies
  - practices for handling the personal data of EU residents
  - the organization's privacy compliance infrastructure (to ensure it satisfies the GDPR's accountability requirements)

fogler rubinoff

THE GDPR AND PIPEDA "ADEQUACY" - TRANS BORDER DATA TRANSFERS

fogler rubinoff

NYMITY
innovating compliance

GDPR AND PIPEDA "ADEQUACY" – TRANS BORDER DATA TRANSFERS

- Through PIPEDA and since December 2001, Canada has enjoyed "adequacy" status under EU's 1995 Data Protection Directive
- Adequacy enables transfer of personal data from EU to organizations in Canada that are subject to PIPEDA without having to implement other mechanisms to protect privacy such as model contracts or binding corporate rules
  - A distinct convenience for Canadian businesses especially important under new trade agreements like the Canada-EU Comprehensive Economic and Trade Agreement which will only increase the volume of consumer and employee data flows into Canada from the EU

fogler rubinoff

GDPR AND PIPEDA "ADEQUACY" – TRANS BORDER DATA TRANSFERS

- Canadian organizations that are not subject to PIPEDA (such as universities, public bodies and organizations subject only to provincial privacy legislation) do not benefit from this adequacy status
- Instead, such organizations must ensure they have consent for the transfer or other appropriate safeguards in place before transferring EU personal data to Canada

fogler rubinoff

GDPR AND PIPEDA "ADEQUACY" – TRANS BORDER DATA TRANSFERS

- Canada's "adequacy" status under 1995 Directive based is on evidence that
  - basic consent principles are present in PIPEDA – namely: purpose limitation; data quality & proportionality; transparency; security; rights of access; rectification & opposition; and restriction of onward transfers and
  - PIPEDA provides adequate procedural and enforcement mechanism that promote compliance, help data subjects and offer redress
- GDPR includes new provisions (not in 1995 Directive) that may be considered central principles of data protection – again, such as: erasure; breach notification; data portability; privacy by design & default; right not to be subject to automated decisions; objection to marketing

fogler rubinoff

GDPR AND PIPEDA "ADEQUACY" – TRANS BORDER DATA TRANSFERS

- On May 25, 2018, GDPR will repeal and replace 1995 Directive and change EU's approach to an "adequacy" determination
- GDPR differs also significantly from 1995 Directive in that it specifically directs the European Commission to examine not only the relevant privacy law (e.g., PIPEDA) but also laws regarding public security, defence, national security and crime as well as international commitments … i.e., all of the laws that form Canada's overall privacy framework

fogler rubinoff

GDPR AND PIPEDA "ADEQUACY" – TRANS BORDER DATA TRANSFERS

- Once GDPR in force, Canada's "adequacy" status will be time limited and subject to monitoring by European Commission
  - envisages mechanism for periodic review at least every four years
- If the European Commission ever revokes Canada's adequacy status, it will likely then enter into consultations with Canada to try to address problematical issues
- Losing that status would make doing business in the EU much more difficult for Canadian companies
- Consideration is now being given to amending PIPEDA to maintain Canada's EU adequacy status
  - "*One of the objectives of OPC's review of the consent model will be to ensure Canada's laws remain adequate*." Federal Privacy Commissioner, Daniel Therrien 2016

fogler rubinoff

GDPR AND PIPEDA "ADEQUACY" – TRANS BORDER DATA TRANSFERS

- Some commentators contend that it would be politically difficult for the EU to withdraw adequacy status from Canada
  - It could send a message to other countries that bar is too high and not to bother passing data protection laws
- Instead of waiting for legislative changes, Canadian organizations can take control of their concerns respecting any uncertainty over PIPEDA's continuing adequacy status
  - There are alternatives to adequacy

fogler rubinoff

ALTERNATIVES TO ADEQUACY

- Alternatives to relying on “adequacy" status:
  - Binding Corporate Rules – GDPR explicitly acknowledges as valid (helpful in covering current member states that don’t recognise)
  - Standard Contractual clauses (no longer require prior approval from from DPAs)
  - Approved Code of Conduct per Article 40 – with binding enforceable commitment to safeguards/TOMs (as may be drawn up by associations or other bodies)
  - Article 42 Certifications (seals etc.) – to be further defined and requires enforceable commitment by controller and/or processor to apply safeguards/TOMs
  - Note – explicitly not lawful to transfer data in response to legal requirement from third country

NYMITY
innovating compliance

…AND DEROGATIONS

- NOTE ALL REQUIRE EXPLICIT CONSENT
- The data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards.
- The transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request.
- The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person.
- The transfer is necessary for important reasons of public interest.

NYMITY
innovating compliance

…AND DEROGATIONS

- The transfer is necessary for the establishment, exercise or defence of legal claims.
- The transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.
- The transfer is made from a register that, according to EU or member state law, is intended to provide information to the public and that is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down in Union or Member State law for consultation are fulfilled in the particular case.

NYMITY
innovating compliance

EU-US PRIVACY SHIELD - IMPACT ON CANADIAN BUSINESSES

O'Melveny

EU-US PRIVACY SHIELD COMPLIANCE

- EU Commission has found Canada provides adequate protection, but not US
- Privacy Shield is mechanism that allows for transfer of EU personal data to US (replaces Safe Harbor)
- Must certify adherence to seven core principles:
  - Notice;
  - Choice;
  - Accountability for Onward Transfer;
  - Security;
  - Data Integrity and Purpose Limitation;
  - Access; and
  - Recourse, Enforcement and Liability
- Must update third-party vendor contracts under Onward Transfer Principle
- EU Commission recent review report confirms Privacy Shield continues to ensure an adequate level of protection for personal data

O'Melveny

KEY TAKEAWAYS

- On May 25, 2018, the GDPR *will* replace the 1995 Data Protection Directive and the eP Reg *may* replace the ePrivacy Directive (although most don't expect the eP Reg to become law until 2020)
- Many Canadian organizations will be subject to the GDPR
- Many Canadian organizations will also be subject to the eP Reg

fogler rubinoff NYMITY innovating compliance O'Melveny

KEY TAKEAWAYS

- The GDPR is different in many important respects from PIPEDA including
  - It places greater obligations on organizations when processing personal data
  - It provides individuals with more rights which are easier to enforce
  - It changes and increases the risks of data protection compliance

fogler rubinoff

NYMITY innovating compliance

O'Melveny

KEY TAKEAWAYS

- Canadian organizations should:
  - determine whether they will be subject to the GDPR, and if so
    - not rely solely on compliance with PIPEDA as sufficient for compliance with the GDPR … potentially huge financial penalties for non-compliance
    - take steps now (if they haven't already) to prepare for compliance with GDPR, which include getting appropriate legal and technical advice

fogler rubinoff NYMITY innovating compliance O'Melveny

KEY TAKEAWAYS

- Canadian organizations should also determine whether they will be subject to the eP Reg
- Compliance with GDPR and the eP Reg will likely be more complex than many Canadian organizations realize
- It will require a sustained multi-disciplinary effort (including privacy, legal, technology, human resource professionals), careful planning and great determination to succeed

fogler rubinoff NYMITY innovating compliance O'Melveny


KEEP
CALM
AND
PREPARE FOR
THE GDPR

QUESTIONS?

Disclaimer: This presentation contains general information only and does not constitute legal advice. Qualified EU legal counsel should be consulted to assess the application of EU laws to specific facts.

fogler rubinoff

NYMITY
innovating compliance

O'Melveny