Association of Corporate Counsel
GREATER PHILADELPHIA

INTERNATIONAL DATA PROTECTION

April 24, 2019 In-House Counsel Conference

Helen Davenport, Director and Brent Arnold, Partner, Gowling WLG
Debra Bromson, Assistant General Counsel, AAA Club Alliance Inc

Follow us on social media!

@accgp @delvacca www.acc.com

April 24, 2019 In-House Counsel Conference

Introduction

- Inescapable global impact of international data regulations on international business operation and risk
- In this session we will focus on:

1. US
2. Canada
3. UK/EU

EXTRA-TERRITORIAL EFFECT

What is meant by “extra-territoriality”?

- Most countries’ data protection laws have broad jurisdictional reach
- Companies do not need to be located in a country to have obligations under the law
- The basis for jurisdiction varies but may include *“conducting business”* or a *“substantial connection”*
- Private (i.e. contractual) obligations also raise foreign law compliance issues

Why does it matter?

- Enforcement risk arising from additional or dissimilar obligations
- Reputational risk & joint investigations
- Avoiding conflicts of laws

When do laws have extra-territorial effect?

Canada

1. PIPEDA applies where there is a *"real and substantial link to Canada"*
2. In practice, applies to collection, use and disclosure of personal information of Canadians

United States

1. FTC, California, Other States: *"doing business in" or "collecting personal information of residents"*
2. HIPAA, Gramm-Leach-Bliley: identified institutions & third parties that receive PHI/PI from them

When do laws have extra-territorial effect?

UK/EU

1. EU established organisations.
2. Extra-territorially, to organisations which offer to sell goods or services to or who monitor individuals in the EU.
3. Those subject to EU member state law by virtue of public international law.

When do laws have extra-territorial effect?

Singapore

Every organisation is required to comply with the PDPA in respect of activities relating to the collection, use and disclosure of personal data in Singapore

PDPA applies to organisations (wherever located) that process the personal data of individuals in Singapore

Personal data collected overseas and then transferred to Singapore will also be subject to the PDPA

When do laws have extra-territorial effect?

GENERALLY: NO BROAD JURISDICTIONAL REACH FROM MIDDLE EAST DP LAWS

UAE:

- Extra-territorial application of GDPR applies to UAE businesses that meet threshold
- DIFC, ADGM and DHCC (the Free Zones) DP Laws apply only to companies registered and with operating in the respective Free Zones
- Dubai Data Law applies only to UAE Federal and local Govt. Entities, and UAE individuals and entities engaging with “Dubai Data”

When do laws have extra-territorial effect?

Bahrain:

The PDPL will apply extraterritorially where:

an individual or business not in Bahrain *is processing personal data within Bahrain through means such as their appointed local representatives*, the PDPL would apply.

Qatar:

The DPL does not specify any geographic limitations on its application.

Others:

In GCC counties, sectoral laws only and no extra-territorial applications.

In practice, this means:

- Company with offices/establishments internationally

How we deal with this in practice

1	Starting Point for UK entities: GDPR and DPA 2018 (cross-reference other European countries)
2	
3	
4	
5	

How we deal with this in practice

1	Starting Point for UK entities: GDPR and DPA 2018 (cross-reference other European countries) ✓
2	Decide the level of control over subsidiaries
3	
4	
5	

How we deal with this in practice

1	Starting Point for UK entities: GDPR and DPA 2018 (cross-reference other European countries) ✓
2	Decide the level of control over subsidiaries ✓
3	Implementing rules from other applicable jurisdictions
4	
5	

How we deal with this in practice

1	Starting Point for UK entities: GDPR and DPA 2018 (cross-reference other European countries) ✓
2	Decide the level of control over subsidiaries ✓
3	Implementing rules from other applicable jurisdictions ✓
4	Harmonise rules as much as possible
5	

How we deal with this in practice

1	Starting Point for UK entities: GDPR and DPA 2018 (cross-reference other European countries) ✓
2	Decide the level of control over subsidiaries ✓
3	Implementing rules from other applicable jurisdictions ✓
4	Harmonise rules as much as possible ✓
5	Training / Awareness strategy !!

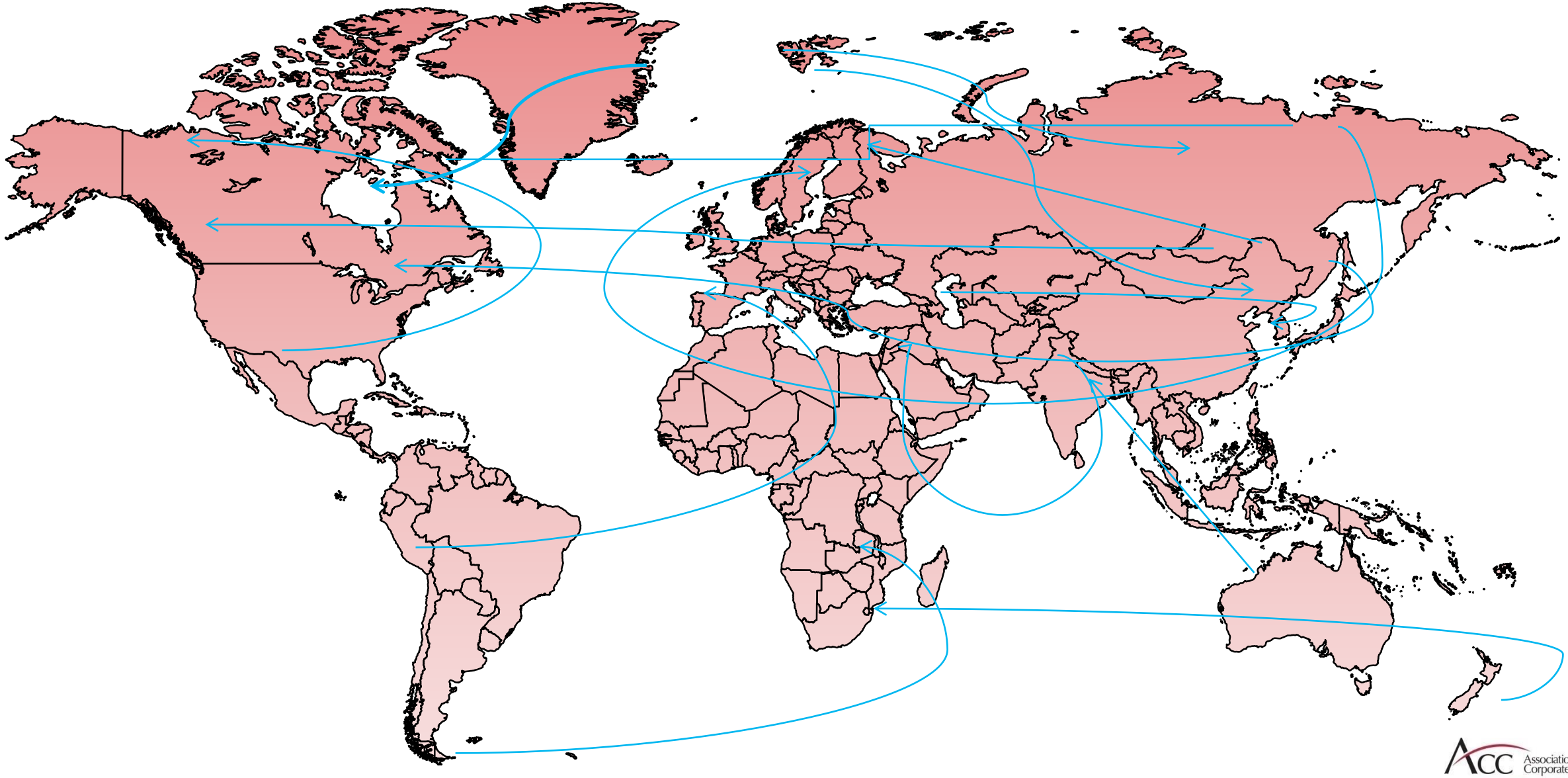
Documentation

- **Tailored documentation:**

1. Data protection policies
2. Training
3. Privacy policies
4. Cookies policies

DATA TRANSFERS AND DATA SOVEREIGNTY

Cross-border transfers of personal data



Data Transfers

Data transfers are fundamental to the business of most companies with operations internationally. Companies may have overseas offices; use a data centre in another country or hire vendors that host data in various locations.

- What are the restrictions on the transfer of personal data in different countries?
- What are the mechanisms to address these requirements?

Data Transfers – Europe (and the UK)

- **Outside of the EEA**
  1. Adequacy decision
  2. Standard Contractual Clauses
  3. Binding Corporate Rules
  4. Privacy Shield

- **Europe to the UK**
  1. See above!

Current state:

- Provinces are either under *PIPEDA* or substantially similar legislation
- Statute, regulations don't expressly require additional consent to share / transfer data across organizations / borders

Current state: *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5 (Federal)

- **Federal Office of the Privacy Commissioner's stance since 2009:***
  - PIPEDA does not prohibit organizations in Canada from transferring personal information to an organization in another jurisdiction for processing.
  - PIPEDA does establish rules governing transfers for processing.
  - A transfer for processing is a "use" of the information; it is not a disclosure. Assuming the information is being used for the purpose it was originally collected, additional consent for the transfer is not required.

*Source: OPC, Guidelines for Processing Personal Data Across Borders, https://www.priv.gc.ca/en/privacy-topics/personal-information-transferred-across-borders/gl_dab_090127/

Current state: *Personal Information Protection Act*, SBC 2003, c 63 (British Columbia, private)

- **Statute covers private / commercial entities**
- **Additional / express consent for transfer not explicitly required**
- **However, personal information must be adequately protected, including through contractual provisions protecting transfer to third parties**

Current state: *Freedom of Information and Protection of Privacy Act*, RSBC 1996, c 165 (British Columbia)

- **Statute covering *public* bodies requires personal information in the custody of public bodies is stored and accessed only in Canada, *unless:***
  - **Individual consents in writing**
  - **Disclosure is pursuant to exceptions under the Act**

Current state: *Personal Information Protection* Act, SA 2003, c P-6.5 (Alberta)

- **Statute covers private / commercial entities**
- **Organizations using service providers outside Canada to use / disclose / store personal info must disclose, in their privacy policies,**
  - **Which countries the data is going to / in**
  - **Purpose for using a provider outside Canada**
- ***And* must provide written notice to an individual *in advance* of the collection / transfer outside Canada**

Current state: *An Act respecting the protection of personal information in the private sector*, RSQ, c P-39.1 (Québec)

- **Anyone communicating personal information to anyone outside Québec must ensure it isn't used / disclosed in a manner that goes beyond the scope of the consent provided by the individual**

Sea Change: *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5 (Federal)

- **Federal Office of the Privacy Commissioner has just announced a consultation to consider whether prior consent is required for all disclosures of info between individuals, including transfers between organizations and their service providers**
- **This would include transfers within Canada or cross-border**
- **Proposal *expressly* contemplates express prior consent to disclosure across a border**

*Source: Gowling WLG, *Federal Privacy Commissioner Proposes A Complete Reversal of its Longstanding Approach to Data Transfers, Including Cross-border Transfers*, https://gowlingwlg.com/en/insights-resources/articles/2019/federal-privacy-commissioner-proposes-reversal/

Sea Change: *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5 (Federal)

- **Public consultation will be open until June 4, 2019**
- **A change in the law will create practical challenges for organizations:**
  - navigating the conflicting requirements of vastly divergent privacy regimes in different sectors and jurisdictions across the country, in particular with respect to the processing of personal health information;
  - creating workable policies and procedures to obtain meaningful individual consent for cross-border data transfers to each new service provider; and
  - revising privacy policies and procedures recently updated in compliance with the new *Guidelines for Obtaining Meaningful Consent* to account for a vast number of situations in which additional informed consent would have to be obtained from existing clients and business partners for transfers of information for processing - even in cases where clear individual consent for the processing itself has already been obtained.

*Source: Gowling WLG, *Federal Privacy Commissioner Proposes A Complete Reversal of its Longstanding Approach to Data Transfers, Including Cross-border Transfers*, https://gowlingwlg.com/en/insights-resources/articles/2019/federal-privacy-commissioner-proposes-reversal/

Data Transfers – US

- If transferring within the US, a company should disclose in the privacy policy how the company shares personal data, but most state laws don't apply to this.

- CCPA: If the company collects information from a consumer in California and "sells" personal information to third parties, must provide a link on their internet or means to enable the consumer to opt out of the "sale".

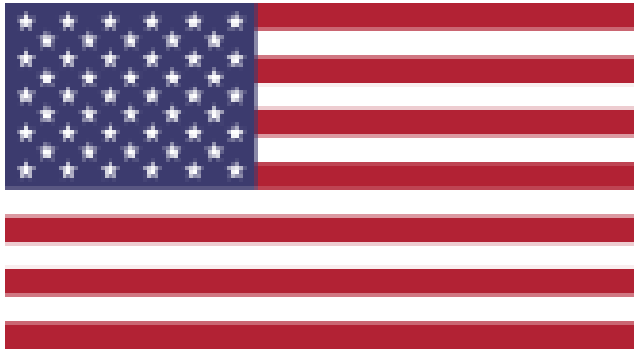
    - A transfer to a service provider to fulfill a business purpose must be governed by a written agreement so it won't be considered a sale.

- If subject to GDPR, and transferring personal data to the EU, to get it back must have in place one of the GDPR requirements—so should transfer data only when you have to

Data sovereignty

Apart from Transfer limitations, are there data sovereignty laws that impose additional legal impediments to cross-border transfers?

Data sovereignty – Canada, US & UK



Managing cross-border data flows

- How does a global company with operations in different parts of the world deal with cross-border data transfers? What are the best practices and pitfalls to avoid?
  - Importance of understanding your data flows
  - Check this issue before you move into new markets, appoint a vendor or use a data centre
  - Keep up to date with changes and ensure that the mechanisms are put in place to meet the legal requirements
  - Cost benefit analysis

INTERNATIONAL DATA BREACHES

Introduction

Notification requirements – 

Canada: Federal Private Sector Privacy Law (PIPEDA)

Notification/Reporting applies to a "breach of security safeguards":

"The loss of, unauthorized access to or unauthorized disclosure of personal information resulting from a breach of an organization's security safeguards that are referred to in Clause 4.7 of Schedule 1 or from a failure to establish those safeguards."

- Personal information is lost, or accessed by an unauthorized individual;
- The loss or unauthorized access is the result of someone violating the organization's security safeguards, or the result of a failure to establish such safeguards.

Notification requirements – 

Key Obligations:

- Determine if the breach poses a “real risk of significant harm” to any individual whose personal information was involved in the breach;
- Notify individuals as soon as feasible of any breach that poses a “real risk of significant harm”;
- Report any data breach that poses a “real risk of significant harm” to the Privacy Commissioner, as soon as feasible;

Notification requirements – 

Key Obligations:

- Where appropriate, notify any third party that the organization experiencing the breach believes is in a position to mitigate the risk of harm; and
- Maintain a record of the data breach and make these records available to the Privacy Commissioner upon request.

Notification requirements –

Canada: Alberta Personal Information Protection Act (PIPA)

- Mandatory breach notification/reporting obligations where an organization determines that a real risk of significant harm exists to an individual as a result of a breach of personal information

Voluntary Notification of Commissioners in BC, Quebec

- Laws do not require notification/reporting but individuals may have been notified under PIPEDA requirements; and may be advisable to voluntarily report to Commissioner in case of inquiries

Notification requirements – 

United States:

- All 50 States and District of Columbia require notification
  - Certain states require service providers/vendors to notify the owner or licensee of the information of a security breach
- Continually changing legal requirements
- Generally limited to defined categories of PI - may or may not include account information, passport numbers, health information and health account information, biometric data
- Most require notification in the “most expedient time possible and without unreasonable delay” - some have specific time limits—the shortest is 30 days
- 29 States require notice to State Agencies but some apply only if a threshold is surpassed (e.g. > 500 affected residents).

Notification requirements – 

United States:

- 3 states require credit monitoring to be provided to residents
- Generally limited to defined categories of PI - may or may not include account information, passport numbers, health information and health account information, biometric data
  - Federal laws require notification for breaches of healthcare information, information from financial institutions, telecom usage information, and government agency information.
- Most require notification in the “most expedient time possible and without unreasonable delay” - some have specific time limits—the shortest is 15 business days
- 30 States require notice to the state government and consumer reporting agencies but some apply only if a threshold is surpassed (e.g. > 500 affected residents).
  - Notice to the Attorney General/Department of Legal Affairs/Office of Consumer Protection/State Police
  - More states also require notice to credit bureaus/consumer reporting agencies (some limit which ones), health services (CA)

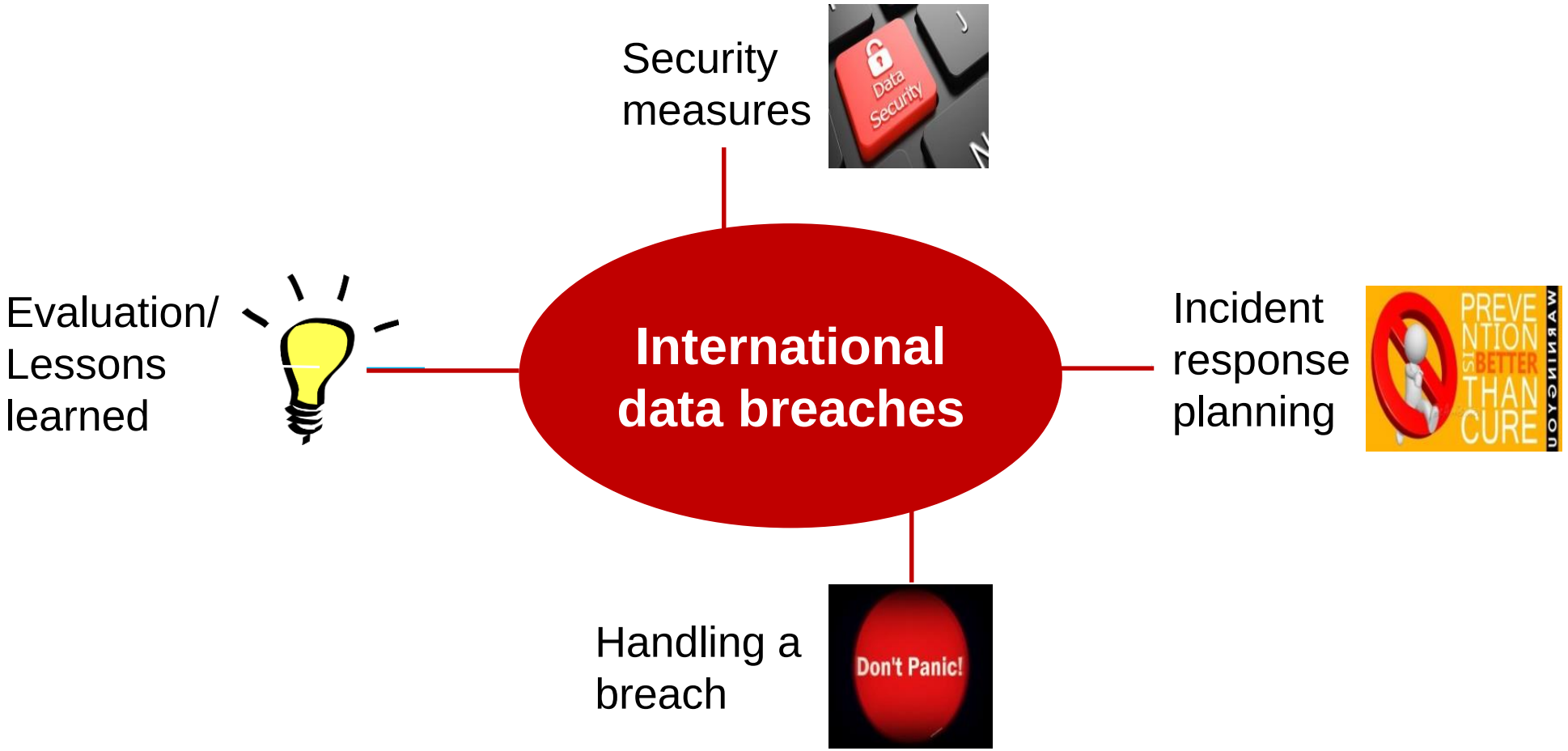
Notification requirements –

Potential breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, **personal data?**

- **Controller's** notification to regulator
  - within **72 hours** if feasible
- **Controller's** notification to data subjects
  - without undue delay
- WP29/EPDB Guidance

- **Processor** to notify **Controller** of breaches - without undue delay

Practical strategies



Conclusions

- Practical aspects on international DP frameworks affecting you as GC's and lawyers of international businesses
  1. Build data maps relevant to your business
  2. Prioritise risk regions
  3. Identify common/baseline compliance elements across jurisdictions
  4. Stay up-to-date with relevant global frameworks
- Digital Protectionism: on the rise and impacting organisations

INTERNATIONAL DATA PROTECTION

April 24, 2019 In-House Counsel Conference

ACC Association of Corporate Counsel
GREATER PHILADELPHIA