GDPR Data Management Controls Readiness

Deborah Henderson

DAHenderson Consulting Inc.

Feb 2018

© 2017 DAHC

Proprietary and Confidential

Disclaimer:
DAHenderson Consulting Inc. (DAHC) is not a law firm and therefore, does not provide legal advice on data privacy regulations (e.g. GDPR); consultants are not lawyers.

The expectation is the audience for this presentation use DAHenderson Consulting Inc. here presented information only, as a foundation for the audience to then enter discussions and leverage their global Legal / Data Privacy experts, often with outside Counsel, to interpret the data privacy regulation / law (e.g. GDPR) impact.

DAHenderson Consulting Inc.'s role is not to provide this advice / guidance, but rather DAHenderson Consulting Inc. has partnered with enterprise global Legal / Data Privacy experts and other key personnel in Data Governance, IT, Risk, Procurement, etc., to translate the global Legal / Data Privacy experts' interpretation into operationalized practices supporting data privacy compliance. DAHenderson Consulting Inc. does not guarantee compliance with any applicable laws and / or regulations (e.g. GDPR) in any jurisdictions (e.g. European Union.) The expectation is that the audience reviews and vets the DAHenderson Consulting Inc. opinions /comments/statements – with an accredited law firm and their own experts for final opinions.

© 2017 DAHC
Proprietary and Confidential

What is the GDPR?

A new European Regulation that governs data protection in all EU Member States.

The General Data Protection Regulation (GDPR) lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.

The European Commission wants to give back the control over personal data to the individual.

The GDPR was **adopted** in April 2016. It entered into force on 24 May 2016 and will be fully applicable as of 25 May 2018. This gives European governments, EU and global businesses two years time to prepare for the changing legislation.

What is privacy?

‘Personal data’ means any bit of information that can lead to identification of an individual.
This includes: email and IP addresses, fingerprints, geolocation data, personal preferences and interests, employees data, etc.

Art. 8 GDPR
1/ Everyone has the right to respect for their private and family life, their home and their correspondence.

2/ There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society

What is processing?

Art. 4.2. GDPR: “Processing means any **operation** or set of operations which is **performed on personal data** or on sets of personal data, whether or not by automated means, such as **collection**, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.”

In other words: **almost every act relating to personal data**. Teach yourself this reflex.

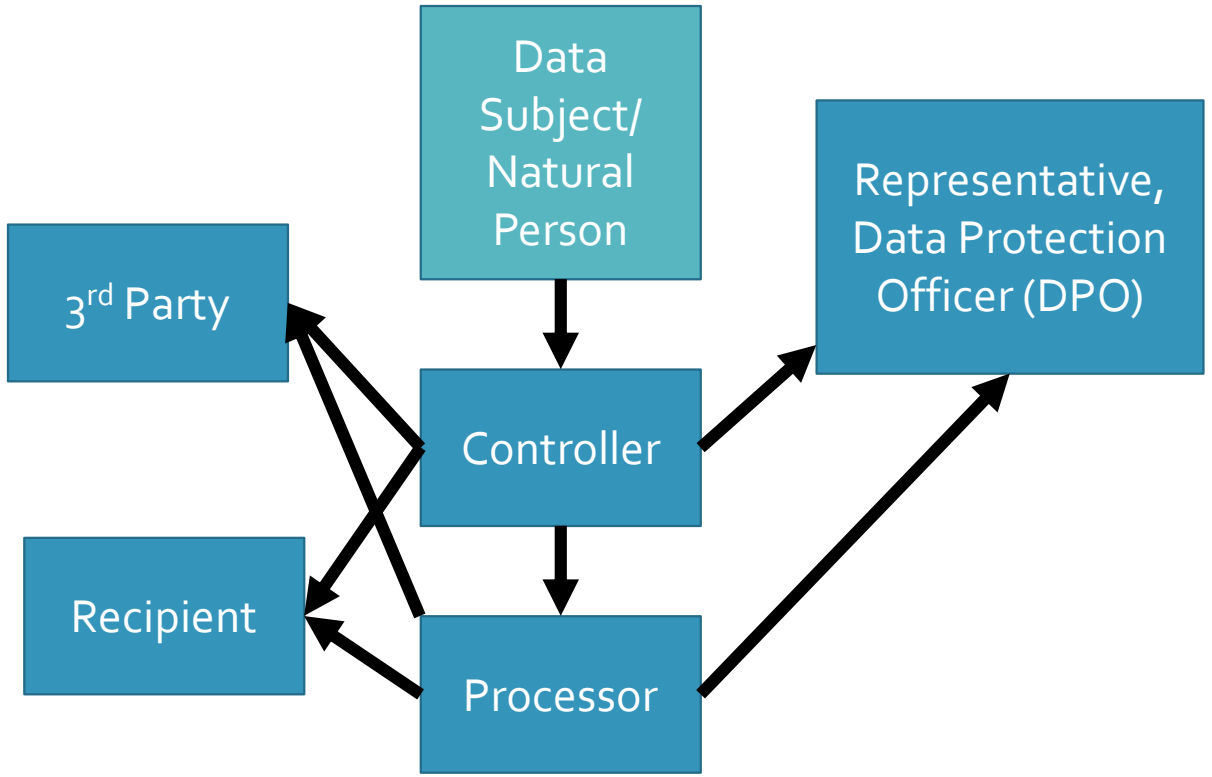
Where does it apply?

"This Regulation applies to the processing of personal data in connection with the activities of an establishment of a controller or a processor in the Union, **regardless of whether the processing takes place in the Union or not**."

(a) the **offering of goods or services**, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

(b) the **monitoring of their behaviour** as far as their behaviour takes place within the Union."

GDPR Defined Roles – Where are you in this?



Considerations include:

- Defining ‘who is who’ in your business model against these roles
- Map to countries the players are located in, where they store the data – laws vary
- Contract language review
- Policies
- Corporate Binding Rules (for conglomerates)
- Internal organization, roles and responsibilities
- Applications and data flows
- Training
- Work behaviours

All parties must comply to GDPR in protection of the Data Subject’s data

What does this mean for non-EU companies?

It **no longer matters** whether or not the data processing takes place within the European Union or not, as long as data of **natural persons in the Union** are processed. This is an important change compared to previous legislation.

Controllers or processors who are not established in the EU should designate, in writing, a **representative in one of the EU Member States**, unless the processing is occasional, does not include processing, on a large scale, of special categories of personal data or the processing of personal data relating to criminal convictions and offences, and is unlikely to result in a risk to the rights and freedoms of natural persons. The representative should, among others things, cooperate with the competent supervisory authorities with regard to any action taken to ensure compliance with the GDPR.

GDPR Impact on Companies

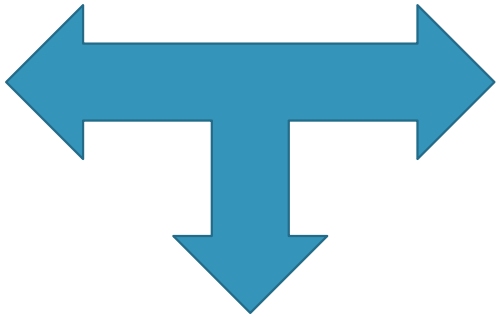
- ✓ Start yesterday, the effort can be many months for some companies to become ‘operational ready’
- ✓ Completion of a Current State Assessment can tell you how big this is for your company
- ✓ GDPR compliance is ongoing and a is culture shift
  - ✓ Communication: there will be organization adjustments
  - ✓ Response Capability includes tech, people, process
  - ✓ Monitor progress towards goals, respond and report to your Board, monitor GDPR changes
  - ✓ This is a permanent program, not a project
  - ✓ Cycle of data protection audit
- ✓ Engage in Certifications, Seals and Marks as appropriate

The result is not only GDPR compliance focused, it addresses customer and employee trust, partner trust, creates positive talking points - ultimately is a marketable record

GDPR themes

Data Subject Rights

- Right to be Forgotten
- Data Subject Consent
- Right of Data Portability
- Right of Access
- Right to Object
- Profiling (Personalization)
- Breach Notification



Tech

- Data Security
- Privacy Impact Assessments
- Retention / Destruction
- Cross-border Transfer
- Pseudonymization

Organization

- Training and Communication
- Privacy Notices
- Codes of Conduct/Certifications
- Organization for GDPR
- Contracts

© 2017 DAHC

Proprietary and Confidential

Exactly what data do I need to protect ?

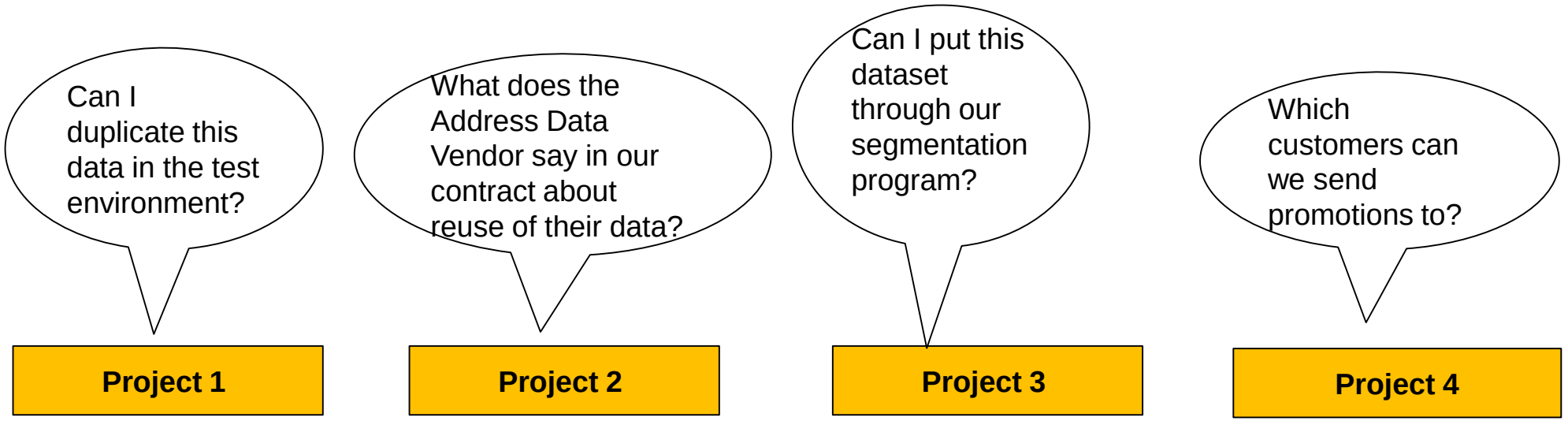
Personal identifying information (also called PII)
"shall mean any information relating to an identified or identifiable natural person ('*Data Subject*'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."

Sensitive personal information (also called SPI)
means personal data consisting of:
(a) the racial or ethnic origin of the data subject,
(b) their political opinions,
(c) their religious beliefs or other beliefs of a similar nature,
(d) whether they are a member of a trade union,
(e) their physical or mental health or condition,
(f) their sexual life,
(g) the commission or alleged commission by them of any offence, or
(h) any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings.

© 2017 DAHC
Proprietary and Confidential

Customer Perspective

IT Perspective

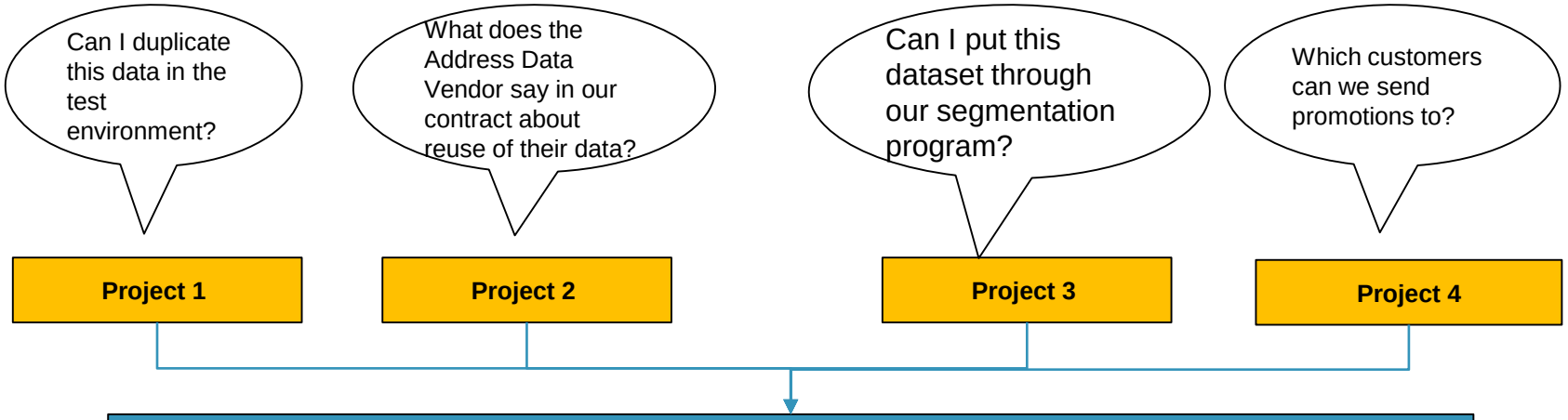


A word on profiling and analytics

Art 4.4 GDPR - data processing may be characterised as “profiling” when it involves (a) **automated processing** of personal data; and (b) using that personal data to evaluate certain **personal aspects** relating to a natural person, in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements.

1. The data subject has the right **not to be subjected** to a decision based solely on automated processing, including profiling, that has legal consequences for him or her or otherwise affects him or her to a significant extent.
2. The data subject has the right **to be notified** of profiling taking place and the purposes and consequences of such profiling.
3. The data subject has the right **to object to profiling** at any time and this option to do so should be communicated clearly to him or her.
4. Profiling that concerns **categories of special data** will be subjected to strict conditions, but waiting on guidance from the European Data Protection Board in this regard. Safest: obtaining **explicit consent**.

Managing Customer and IT Perspectives with Governance

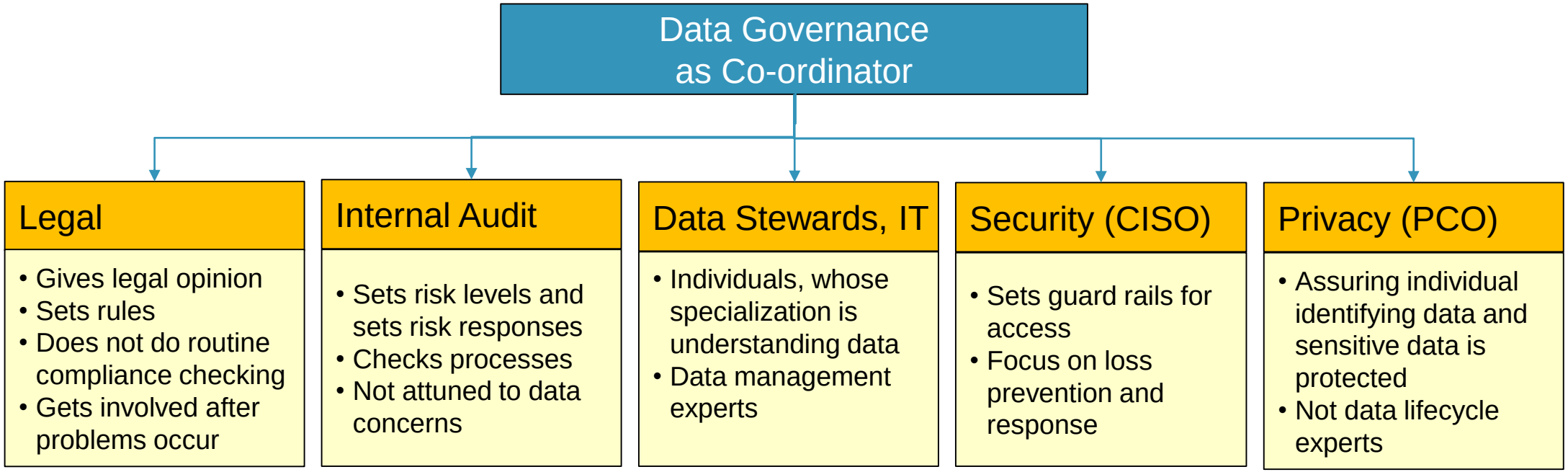


Ongoing Governance

- GDPR Principles based
- High level advisory and coordination for company accountability and record of activities on personal data
- Not data experts, but will reference data experts advice and input
- Will approve organization actions re personal data (Privacy Impact Assessments)
- Track customer and employee questions and responses
- Coordinates breach response
- Assesses risk, authorizes audit

Why You Need a Centralized Data Governance Function

Data Governance partners with other organizations to make sure all parties are talking, decisions are fully informed on data handling and data lifecycle management (acquisition through ultimate disposition). Existing Data Governance can strike this up as a new focus area or domain.



Where to Start

A Current State Assessment and Inventory is the place to start to establish gaps

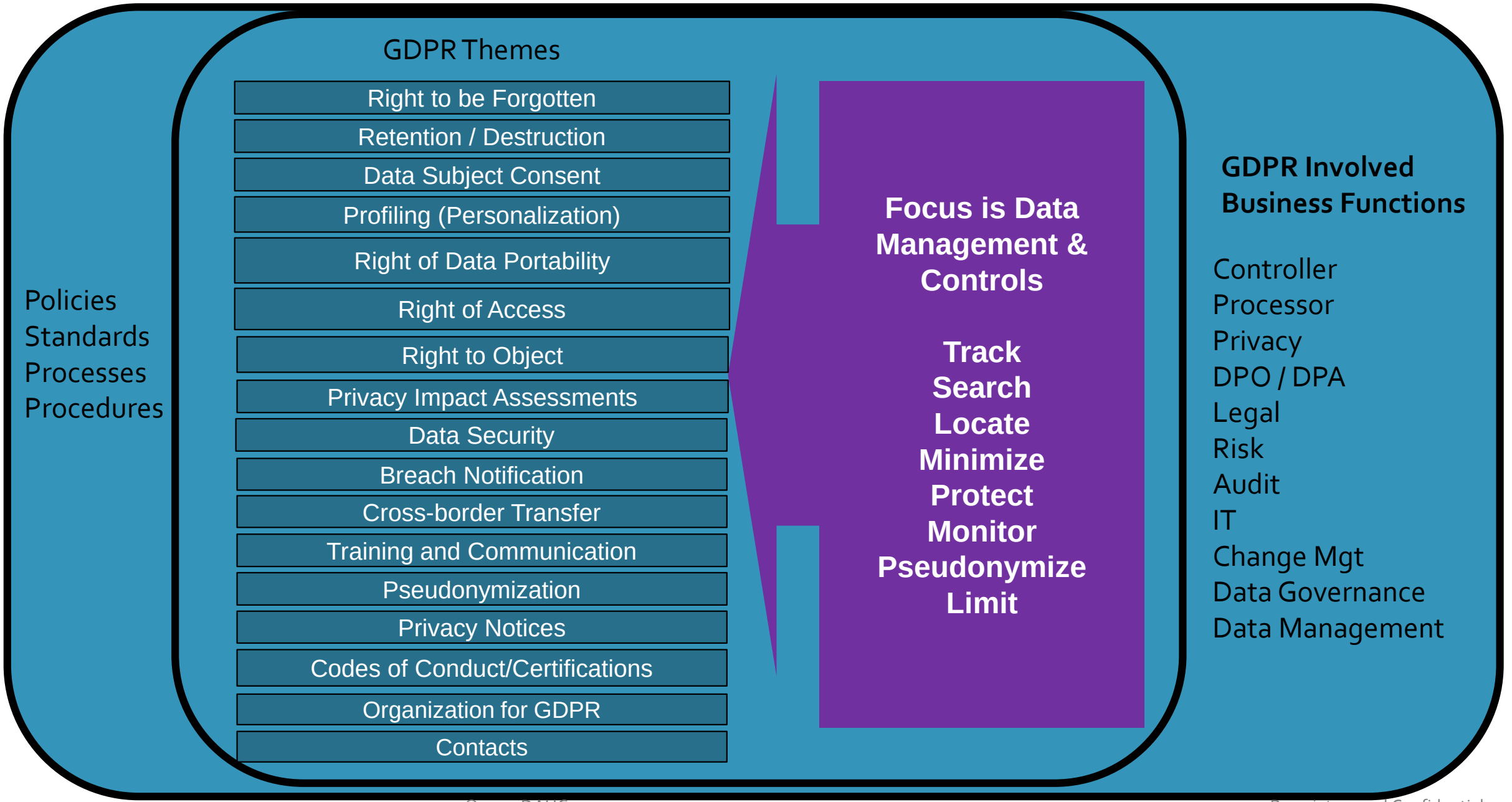
Example questions include:

What PII and SPI data do we collect?
Where are they defined? Where are they stored (business definitions and technical links)
Where and how do we process personal data?
Who is in charge of data protection?
How do we currently get explicit consent from individuals to process their data for multiple purposes?
Can we respond to individuals requests for information on their data?
Who do we get data from? (companies, data vendors)
Do we develop and change systems using design approval gates?
Do we have data breach policies, processes, do we perform ‘breach desktop exercises’ ?
Do we have legal advice and input on personal data handling requirements, risk and contracts?

What do the current state gaps mean to us?
Is our company adequately motivated to fill the gaps?

© 2017 DAHC
Proprietary and Confidential

GDPR Assessment Framework – Level 0©



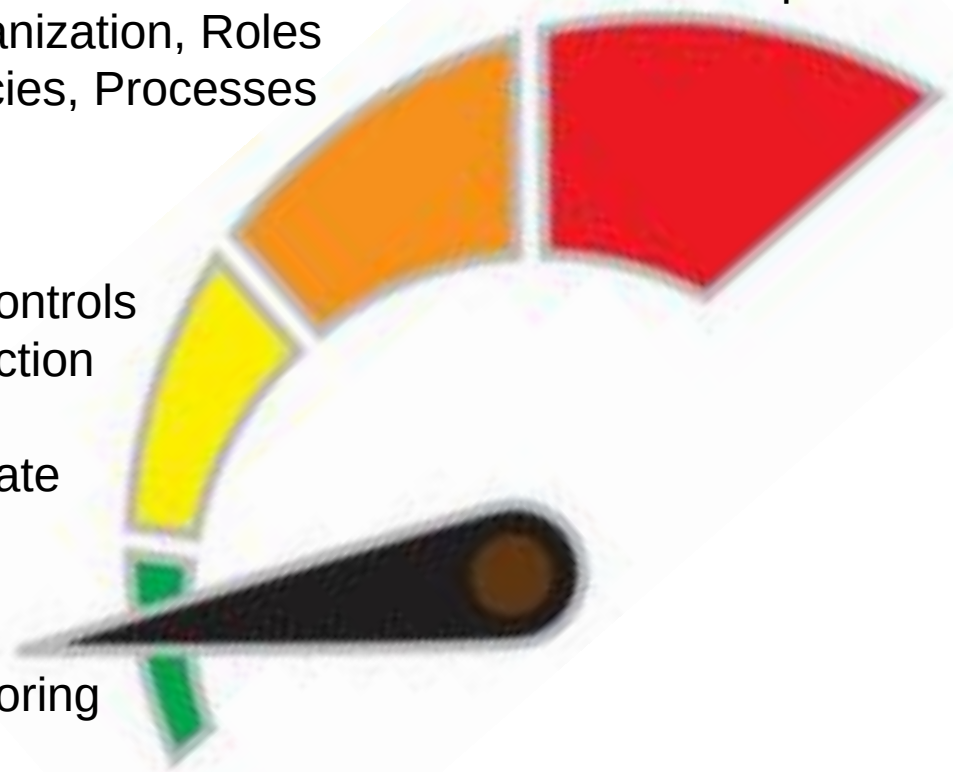
© 2017 DAHC

Proprietary and Confidential

The Way Forward - Getting to Risk Based Compliance

Legal Advice, Contract Changes
Current State Assessment/Gaps
Road Map

Organization, Roles
Policies, Processes



Data Management Controls
Technical Data Protection
Privacy Assurance
Train and Communicate

Implementation
Operations Monitoring
Action Requests
Assessments
Adjustments
Audit

© 2017 DAHC

Proprietary and Confidential

Fluid landscape for Canada and compliance

What PIPIDA does not currently cover that GDPR requires:

1. the GDPR requires that an organization notify regulators and affected individuals *within 72 hours*
2. Under the GDPR a data protection impact assessment is a mandatory pre-requisite before processing personal data for operations that present particular privacy risks to individuals due to the nature or scope of the operation (under Canadian privacy law, privacy impact assessments have generally only been required in the public sector, not in the private sector)
3. The GDPR contains increased transparency obligations – privacy notices to employees, for example, will need to include much more detailed information than is typically provided under *PIPEDA*
4. The GDPR sets out a statutory "right to be forgotten" which would allow employees the right to require their employer to delete data files relating to them if there are no legitimate grounds for retaining the data.

And more…..

https://blogs.dlapiper.com/privacymatters/canada-what-will-the-european-general-data-protection-regulation-mean-for-canadian-employers/

However… data transfers and Canada

the European Commission issued an **adequacy decision** (2002/2/EC) under the Directive that states that the **Canadian Personal Information Protection and Electronic Documents Act** (PIPEDA) assures adequate protection for DATA TRANSFERS. This remains in force until amended, replaced or repealed, which has not been done yet.

Authorizations of transfers made under this Directive will remain valid/remain in force until amended, replaced or repealed.

Canada's participation in the **Five Eyes** intelligence-sharing program with the U.S., U.K., Australia and New Zealand is a major reason why Canada's adequacy status would be in jeopardy. It's no secret the EU has been displeased with the secrecy surrounding government access to data in such jurisdictions.

Seeing the importance of potential sanctions, it is advisable to check GDPR adequacy ruling regularly.

https://iapp.org/news/a/could-canada-lose-its-adequacy-standing/

DAHenderson Consulting Ltd

Thank you for your interest!

Questions and comments can be addressed to:

Deborah Henderson

deborah.henderson@rogers.com

DHender