What Are Companies Doing About GDPR? Is Your Company Ready?

DAMA Day - June 21, 2018

Topics for Discussion

- How are organizations **meeting GDPR requirements**?
- What are the **challenges**? Why is it **hard and expensive**?
- Applying lessons learned: A **practical implementation framework** for meeting GDPR requirements

GDPR In a Nutshell

All about protecting customer data, which means:

- **Knowing where** protected classes of customer data are **being stored**
- **Applying** data protection **controls** on them
- **Using** them only when needed
- **Keeping** them only as needed
- **Deleting** them at request
- **Sharing** them at request
- **Knowing** when they are misused / lost
- **Notifying / responding** when they are misused / lost

Protected Classes of Data

- Basic **identity** information such as **name**, **address** and **ID numbers (PII or personally identifiable information)**
- **Web** data such as **location**, **IP address**, **cookie data** and **RFID** tags
- **Health** and **genetic** data
- **Biometric** data
- **Racial** or **ethnic** data
- **Political** opinions
- **Sexual orientation**

How Are Companies Addressing GDPR

A Risk and Controls Framework for GDPR Readiness

Policy & Governance Controls

- ✓ Hiring Key Corporate Officers
- ✓ Inventorying Data Processors
- ✓ Updating Privacy Policies
- ✓ Revising Data Protection Contracts with Suppliers
- ✓ Upgrading Incident Response Procedures

Data Controls

- ✓ Identifying Sources of Protected Data
- ✓ Mapping Sources to Business Functions / Uses of Data
- ✓ Implementing Technical Protection Controls at Sources based on Data Usage / Function

Policy & Governance Controls

Hiring the Right Officers

1. Have you formalized the titles for **Data Controller** and **Data Privacy Officer**?
2. Have they been staffed?
3. Are their responsibilities and organizational structures clear?

Inventorying Data Processors

1. Are all **Data Processors** within a company identified?
   - Implies that we know **where customer data is stored throughout the enterprise**, and all Business and IT owners (in-sourced or outsourced) are identified

Policy & Governance Controls

Updating Privacy Policies

1. Does it provide the **identity** and contact information of the **Data Privacy Officer**?
2. Does it describe the **purpose** for storing customer data, and **how it will be used**?
   - ★ **CRITICAL**: Purposes and uses need to be **linked** to **business functions** and operations
3. Does it describe what **categories of personal data** are being collected?
   - ★ **CRITICAL**: Categories need to be linked to **Business Glossaries** / **Data Dictionaries**
4. Does it describe **who** data is **being shared** with?
5. Does it describe **how long** data will be **maintained** (and how this was determined)?
6. Does it lay out the customer's rights (to be **forgotten**, to lodge complaints)?
7. Does it describe **what happens** if there is a **breach** and what the **consequences** of **non-compliance** are?

Policy & Governance Controls

Revising Data Protection Contracts with Suppliers

1. Revisiting **who** in the Data Processors' org **can access customer data**
2. Revisiting **incident notification** responsibilities
3. Revisiting **liability claims** and **insurance** requirements
   - This is typically the most challenging area

Upgrading Incident Response Procedures

1. Can you meet the **72-hour timing window** to notify clients of breach or misuse of data?
   - Implies strong data leakage and security event monitoring technical controls for all sources of protected data within all Data Processors
   - Implies comprehensive customer notification / escalation capabilities

Data Controls

Identifying Sources of Protected Data

1. Have you defined Protected Data into **Critical Data Elements (CDEs)** in your Data Dictionary?

Protected Data Class	Critical Data Element (CDE)
Identity Information	• First Name • Last Name • Home or Physical mailing address • …
Web Data	• IP address • MAC address • Website URL • …
Health and Genetic Data	• Prescription • Medical ID / record number • Admit Date • …

2. Have you inventoried all **Sources of CDEs** front to back – mapping business apps to data classes (**logical** to **physical**)?

Data Controls

Mapping Sources to Business Functions / Uses of Data

1. Have you defined a **Functional Taxonomy** (function model), which maps to the uses of data?

Functional Category	Function
Sales and Marketing	• Market Research • Advertising and Promotion • New Customer Acquisition • …
Customer Lifecycle Management	• Onboarding and KYC • Customer Relationship Management • Customer Support • …
Product Management	• Product Selection and Promotion • Product Strategy • New Product Development • …

2. Have you **mapped Sources** of data (business apps) **to functions**?

Data Controls

Implementing Technical Protection Controls

1. Encryption (in flight, at rest)
2. Access control (authentication, authorization)
3. Archival and Retention (information lifecycle management)
4. Deletion (for individual records and database values)
5. Distribution / Sharing
6. Monitoring / Incident Detection (leakage, security event)
7. Escalation (notification, communication)

Goal is to map control types to functions, data and systems in order to measure compliance

What are the Emerging Best Practices?

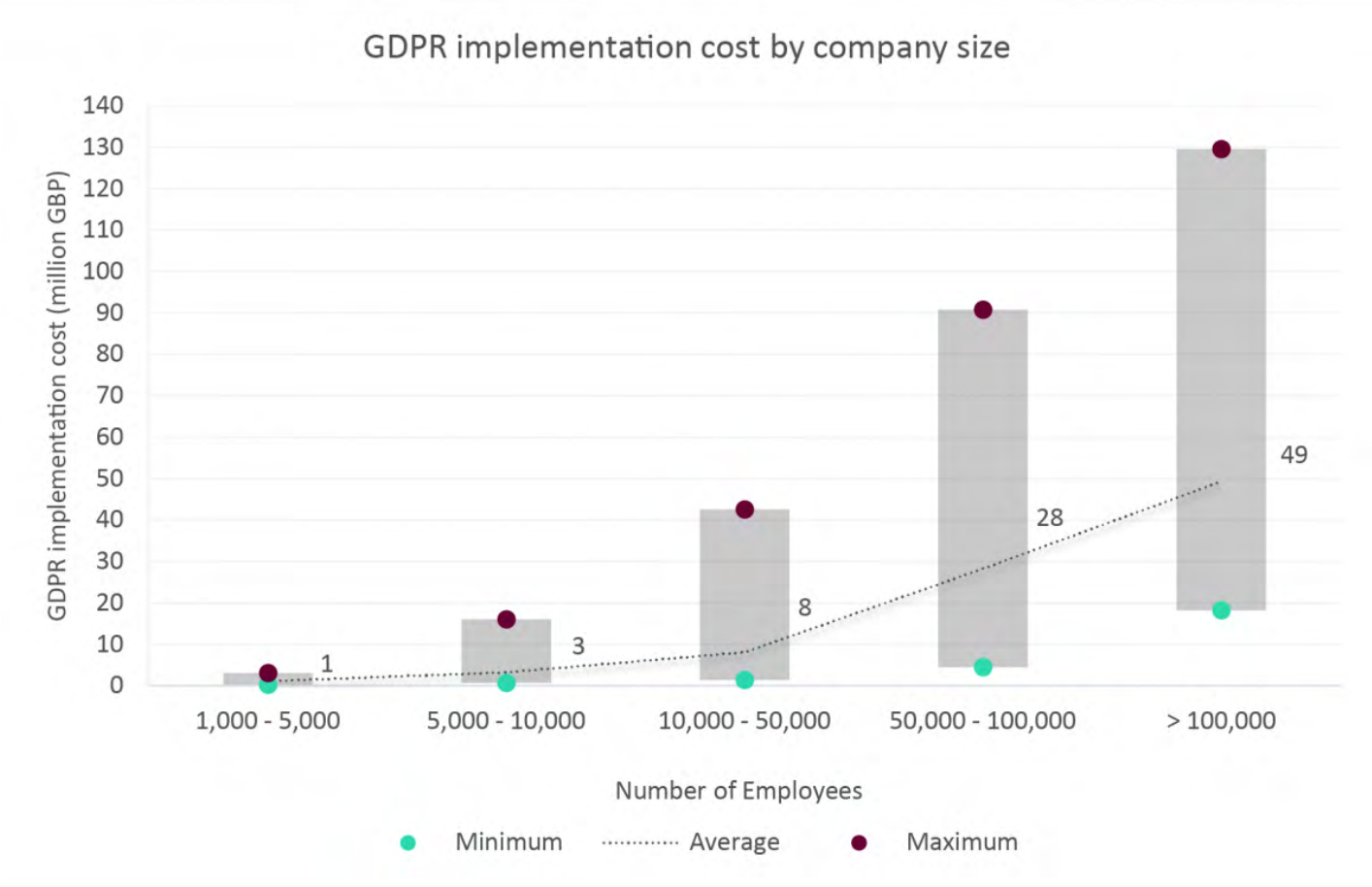
Reusable Simple Enterprise Models

- Either invest in modeling controls, functions and data relationships
- Or, invest in Knowledge Graphs or semantic ontologies (e.g., FIBO, RDF, commercial models)

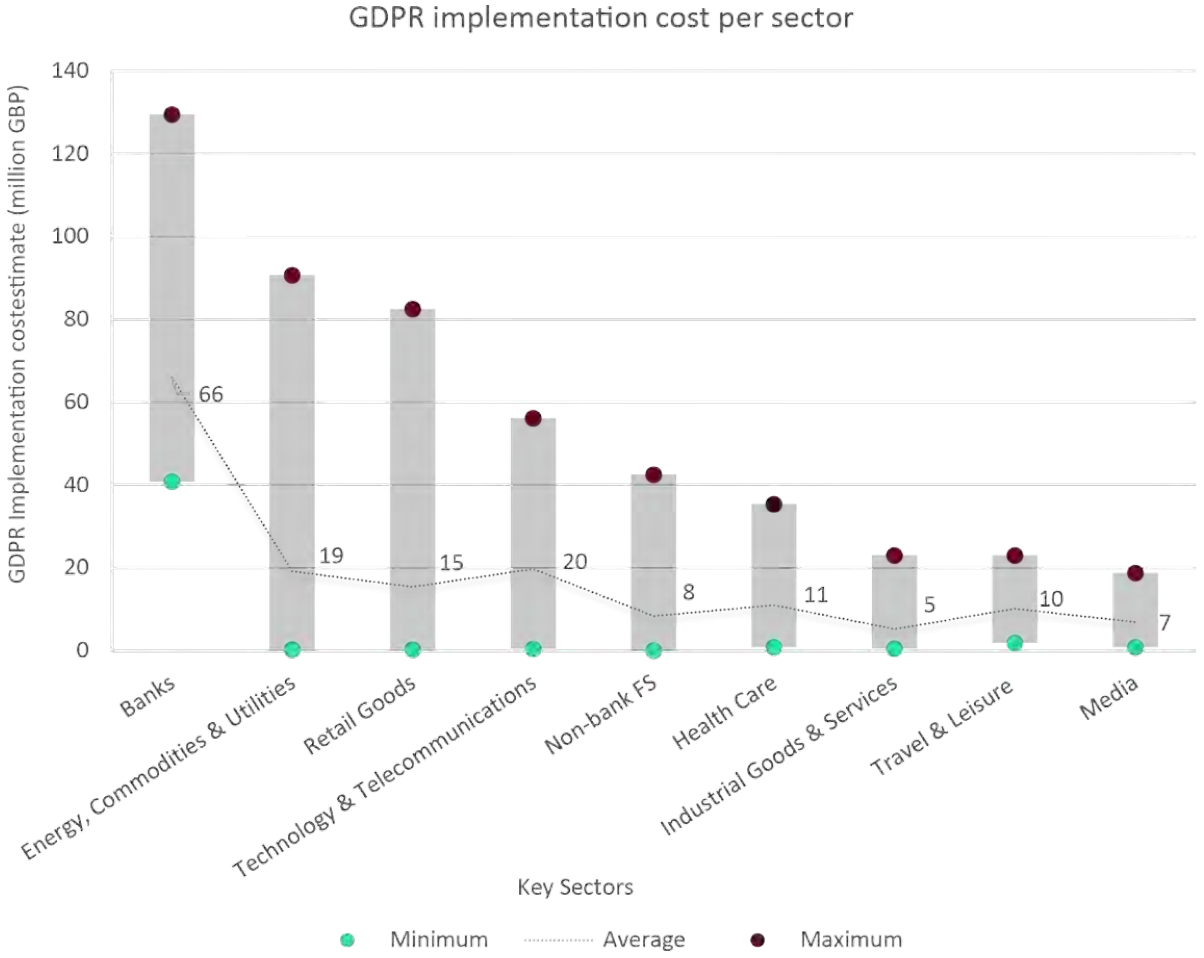
Automated Harvesting

- Adaptors to build inventories of data and meta-data across ecosystem of business apps
- Inference engines and machine learning classification models that map data from business apps to semantic models

How Much Investment is Required?



How Much Investment is Required?



What Are the Key Challenges?

1. Identifying list of **Data Processors**, and renegotiating liability and insurance clauses related to management of customer information

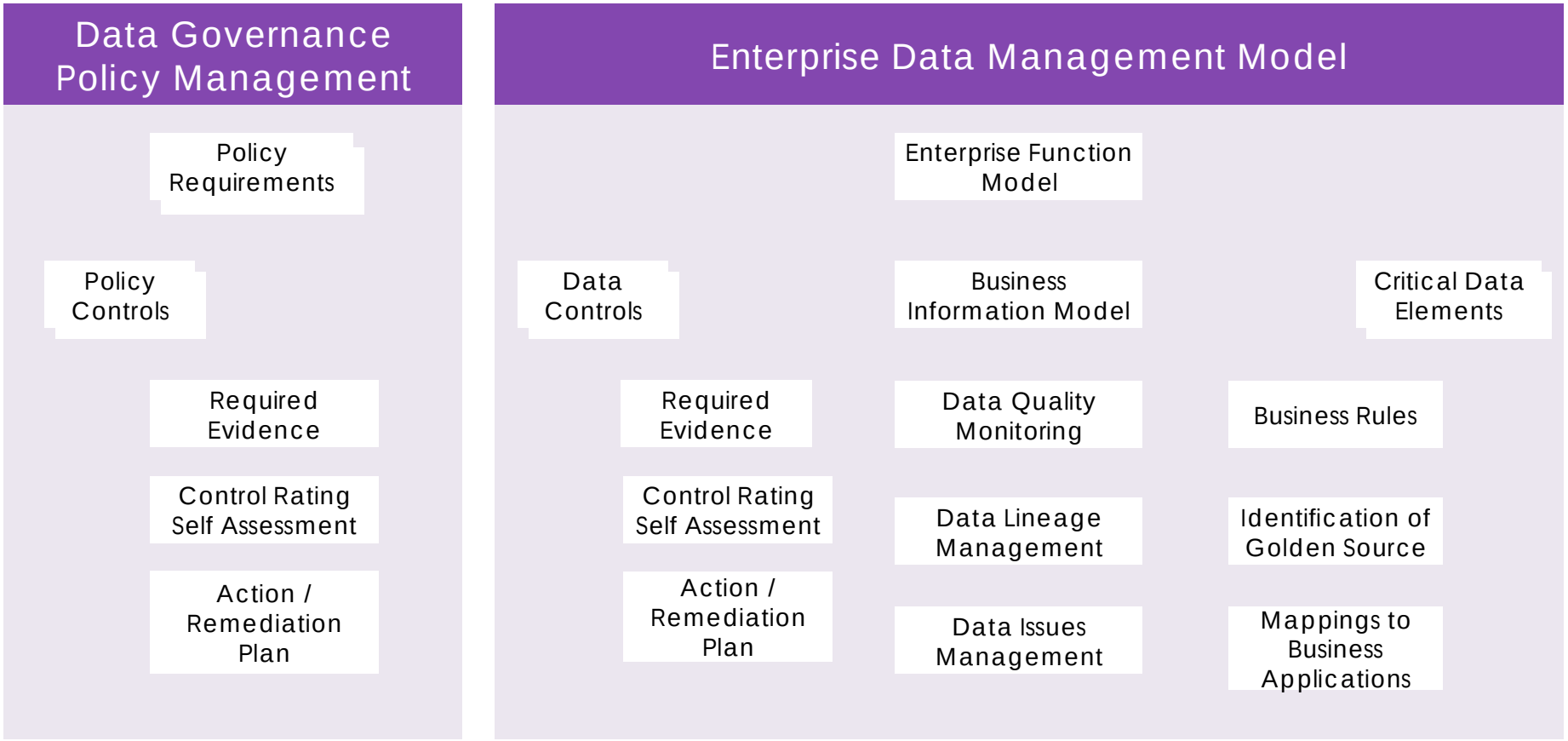
2. **Modeling** of business functions, data classes and required controls

3. Comprehensive **identification** of **in-scope systems**

4. **Implementation** of **adequate technical data protection controls** within in-scope systems – especially for Customer Right to Forget

A Path Forward

The Adaptive Data "Bank in a Box" Meta-Model



Adaptive "Bank in a Box"

- Data Governance in a Box, for the Banking industry
- Comes with **Data Management policies** pre-defined for the most significant regulations
- Comes with definitions of **Banking business functions, information and data models**, and insight and knowledge of which functions create and consume data
- Comes with pre-defined descriptions of **Critical Data Elements** for regulatory functions, as well as the core **business and technical rules** required to attest to their quality

Thank you.

Jeff Goins

Jeff.goins@adaptive.com