Preparing for the EU General Data Protection Regulation
What you need to do, when you need to do it

John Bowman, Senior Principal

Promontory Financial Group, London, UK

Professional Strategies – S21

Agenda

1. **What is the GDPR?**
2. **What to do, when to do it**
3. **GDPR exercise**
4. **Q&A**

Session objectives

- This session will provide an overview of the key impacts that the GDPR will have on businesses that process the personal data of EU residents
- There will be a focus on what the GDPR means for North American-based data controllers and processors and what businesses can do to prepare for the new rules
- There will be an update on the state of play in GDPR negotiations
- There will be a scenario-based exercise which will highlight key issues that need to be considered in the context of the GDPR
- Delegates should take away an improved understanding of the technical and organizational measures they should adopt in order to be compliant with the GDPR

1. WHAT IS THE GDPR?

New rules for the digital age

General Data Protection Regulation (GDPR) is the first comprehensive overhaul of European Union data protection rules in 20 years - it will repeal and replace Directive 95/46/EC

Directly applicable rules (in EU)

GDPR will be directly applicable in all EU Member States, adopted in EEA, and will replace existing national law implementations of the current Directive

A live negotiation

GDPR remains under negotiation but political agreement is expected in late 2015 or early 2016, with a subsequent two year transition period before the new rules go live

Worldwide territorial scope

GDPR will apply to data controllers that process the personal data of EU residents, regardless of location

Enhanced rights, additional obligations

New rules on consent, access rights, profiling, impact assessments, data transfers, and much more

A new regulatory approach

Lead authority model, multilateral approach to transnational cases, new European Data Protection Board

Big sanctions

Maximum fine levels of up to 5% of worldwide enterprise turnover

Will we get consistency?

YES

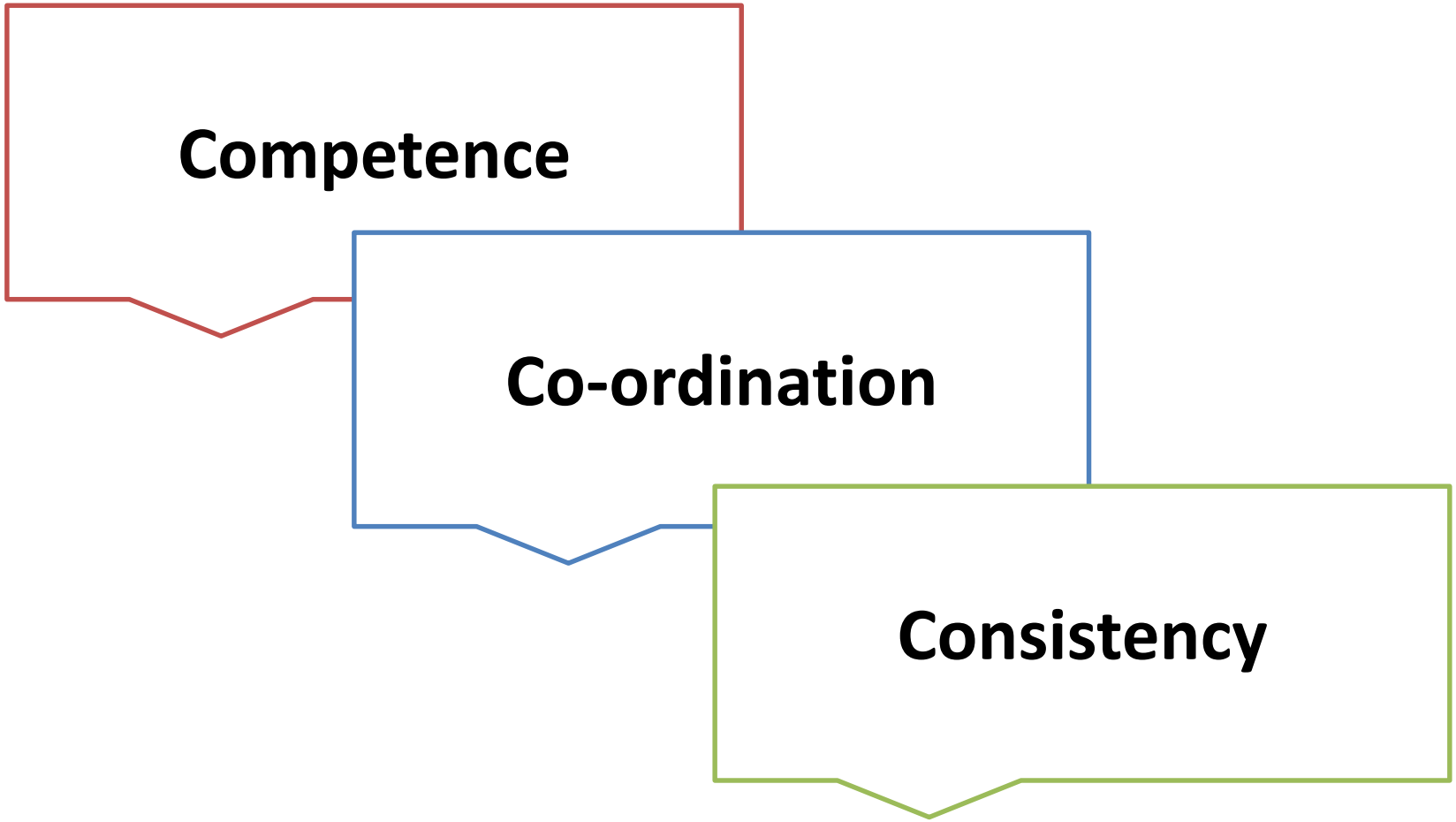
- A **Regulation** has to be applied directly: theoretical consistency in most areas
- The **European Data Protection Board** will own the consistency mechanism and may have own agenda
- The **European Court of Justice** will continue to make pan-European rulings
- The **Commission** can adopt **delegated and implementing acts** but uncertainty on scope and timing.

Will we get consistency?

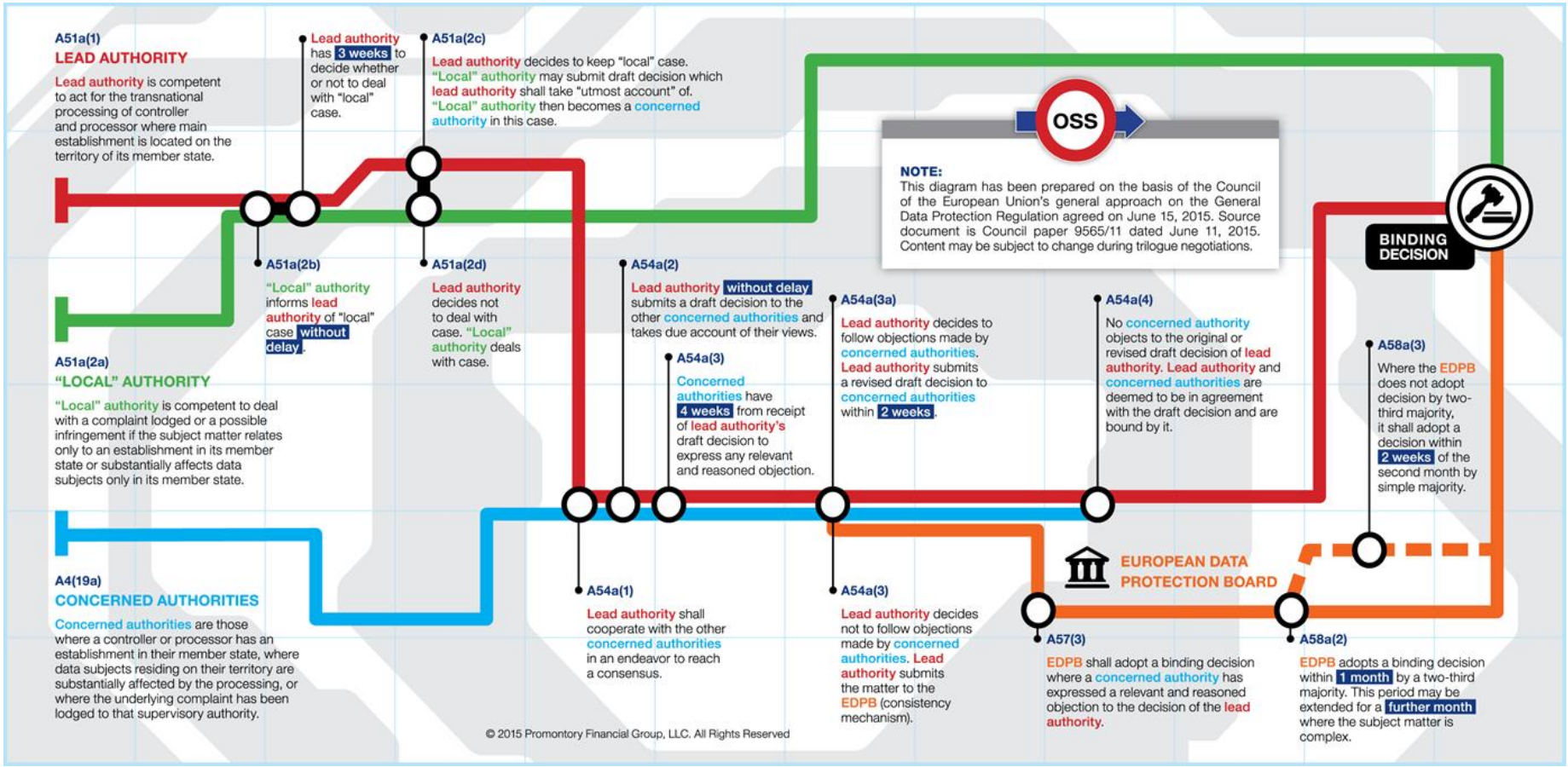
NO

- Some **opt-outs and member state flexibility in Regulation** (e.g. freedom of expression, public sector, employment, research)
- **Local Data Protection Authorities** will still interpret the Regulation in their guidance and enforcement actions
- **Cultural and social norms** will still differ, affecting press coverage, consumer reaction etc

One-stop shop: the ‘three Cs’



A one-stop shop?



Summary: what is the GDPR?

- New rules for the digital age
- Extra-territorial scope beyond the EU
- Consistency, but not all the time
- New regulatory framework
- Big sanctions

2. WHAT TO DO, WHEN TO DO IT

Grounds for processing and transferring personal data

Data controllers will need to choose which grounds for processing and transfer they will rely upon

Explicit consent, contract, legitimate interest,

Adequacy, contracts, BCRs and the 'anti-FISA clause'

Enhanced rights

The data protection rights of EU residents will be enhanced. Controllers and processors will need to fulfil these enhanced rights

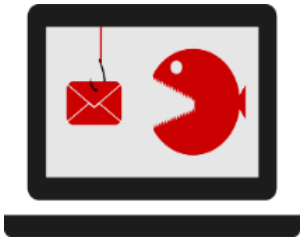
Data portability and access rights

Measures based on profiling

Right to be forgotten

New obligations

Many new obligations will apply to data controllers and processors

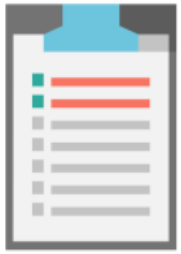


Data protection by design and default

Security of processing

Data Protection Impact Assessments

Breach notifications



Data Protection Officers

Differences between current and new rules

Application: under DPD, member state law applies where entity is established or if established outside EU where processing takes place.

GDPR applies where goods or services are offered to EU residents. If no establishment in EU, then representative must be appointed

Notification of processing abolished: Requirement under DPD but abolished under GDPR. Instead documentation needed to demonstrate compliance

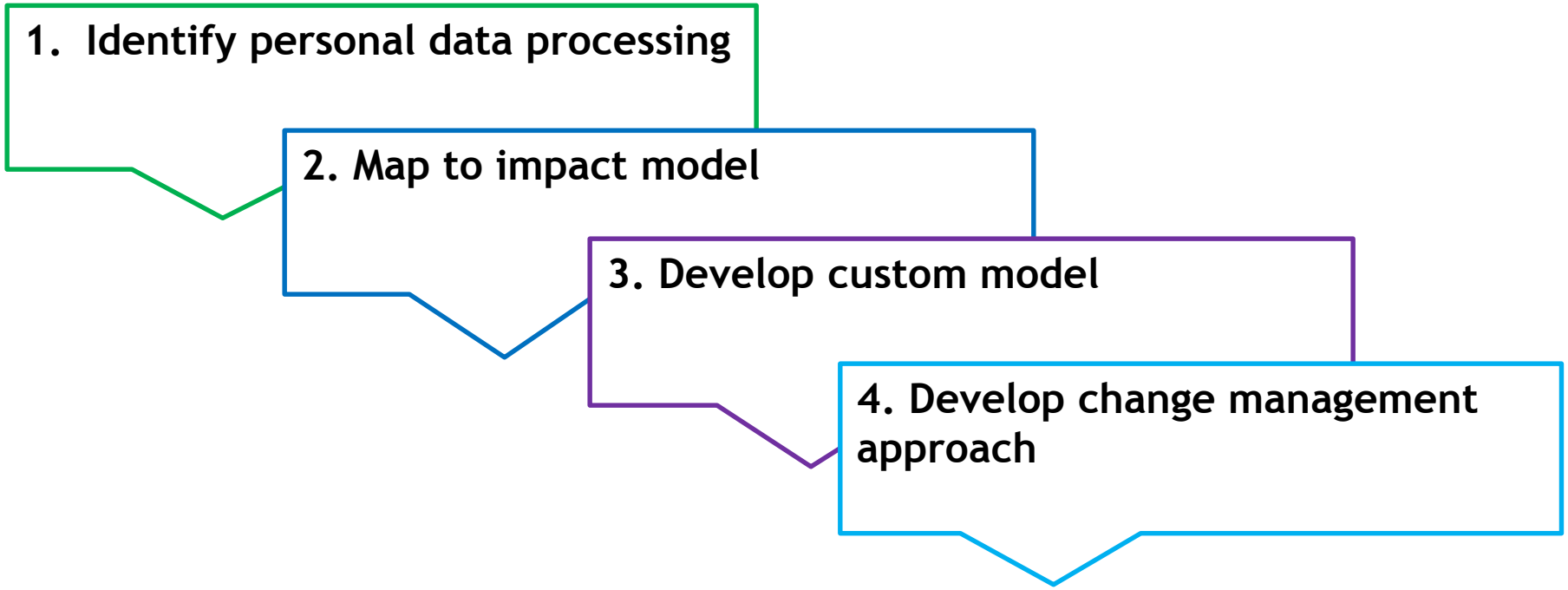
Controllers and processors: DPD generally applies to controllers with processor responsibilities set out in contract. GDPR will also directly apply to processors who could be subject to enforcement action

Pseudonymisation: New to GDPR, pseudonymisation of data can be a protection enhancing measure but pseudonymous data is still personal data

Length: 34 articles in DPD, 91 articles in GDPR

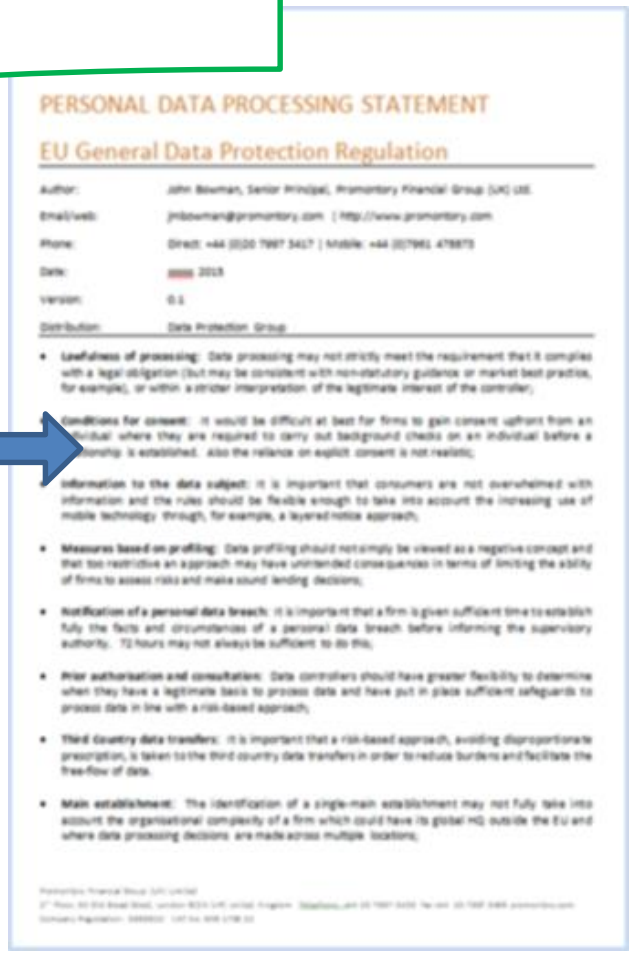
Preparing for the GDPR

The GDPR is complicated. We recommend a four stage approach to preparing for change and managing the transition



1. Identify personal data processing

Personal data processing statement



PERSONAL DATA PROCESSING STATEMENT

EU General Data Protection Regulation

Author: John Bowman, Senior Principal, Promontory Financial Group (UK) Ltd.

Email/web: jmbowman@promontory.com | http://www.promontory.com

Phone: Direct: +44 (0)20 7997 3417 | Mobile: +44 (0)7961 478873

Date: [redacted] 2015

Version: 0.1

Distribution: Data Protection Group

- **Lawfulness of processing:** Data processing may not strictly meet the requirement that it complies with a legal obligation (but may be consistent with non-statutory guidance or market best practice, for example), or within a stricter interpretation of the legitimate interest of the controller;
- **Conditions for consent:** It would be difficult at best for firms to gain consent upfront from an individual where they are required to carry out background checks on an individual before a relationship is established. Also the reliance on explicit consent is not realistic;
- **Information to the data subject:** It is important that consumers are not overwhelmed with information and the rules should be flexible enough to take into account the increasing use of mobile technology through, for example, a layered notice approach;
- **Measures based on profiling:** Data profiling should not simply be viewed as a negative concept and that too restrictive an approach may have unintended consequences in terms of limiting the ability of firms to assess risks and make sound lending decisions;
- **Notification of a personal data breach:** It is important that a firm is given sufficient time to establish fully the facts and circumstances of a personal data breach before informing the supervisory authority. 72 hours may not always be sufficient to do this;
- **Prior authorisation and consultation:** Data controllers should have greater flexibility to determine when they have a legitimate basis to process data and have put in place sufficient safeguards to process data in line with a risk-based approach;
- **Third country data transfers:** It is important that a risk-based approach, avoiding disproportionate prescription, is taken to the third country data transfers in order to reduce burdens and facilitate the free-flow of data.
- **Main establishment:** The identification of a single main establishment may not fully take into account the organisational complexity of a firm which could have its global HQ outside the EU and where data processing decisions are made across multiple locations;

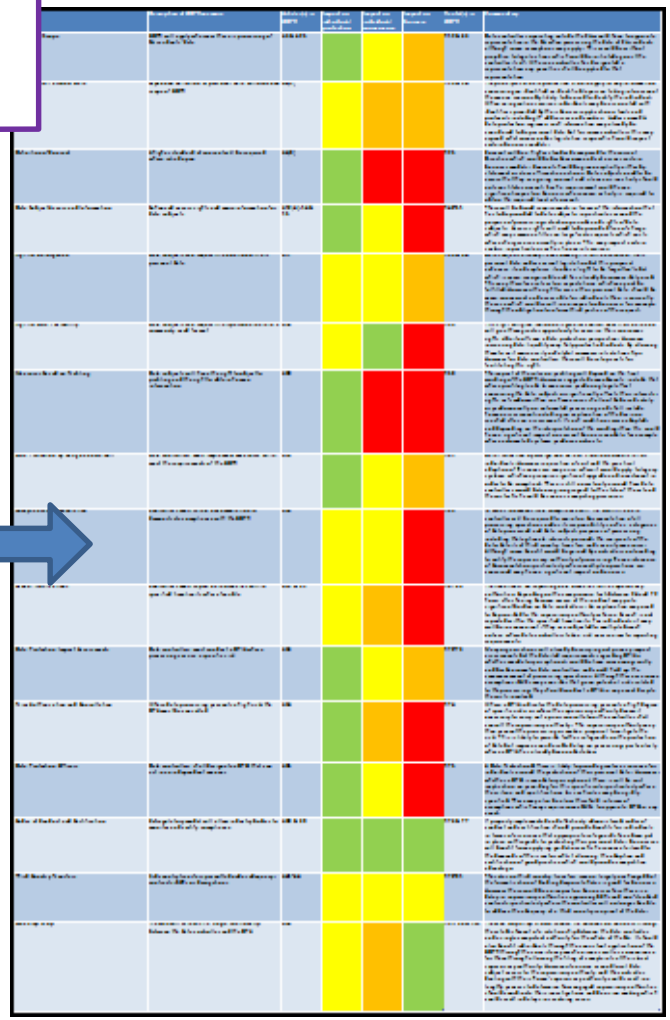
2. Map to impact model

Initial impact analysis

	Rating	Filter1	Filter2	Filter3	Filter4	Filter5	Filter6	Filter7
Significant resource or change may be required to comply	3	3	3	3	3	3	3	3
Moderate resource or change may be required to comply	2	2	2	2	2	2	2	2
Little or no resource or change may be required to comply	1	1	1	1	1	1	1	1
	Reset all	Reset	Reset	Reset	Reset	Reset	Reset	Reset
GDPR Measures	GDPR Article	Online Behavioural Advertising	Conventional Direct Marketing	AML, anti-fraud, sanctions	Social media	Apps	Healthcare	Mean score
Form of instrument	General	1	1	2	1	1	3	1.5
Territorial Scope	3	3	1	3	3	3	1	2.3
Personal data definition	4.2	2	2	2	3	3	2	2.3
Consent: Explicit	4.8	3	3	2	3	3	3	2.8
Main establishment	4.13	1	1	1	2	3	3	1.8
Purpose limitation/data minimisation	5.b & 5.c	3	3	3	2	2	2	2.5
Conditions for consent	7	3	3	2	3	3	3	2.8
Personal data of a child	8	3	1	1	3	3	3	2.3
Special categories of data	9	1	1	3	2	2	3	2.0
Criminal convictions	9.2.j	1	1	3	2	1	1	1.5
Access rights	12.4 & 15	2	2	2	2	2	3	2.2
Information to data subject	14	3	3	2	2	2	3	2.5
Right to be forgotten	17	1	1	1	3	2	1	1.5
Right to data portability	18	1	1	1	3	2	1	1.5
Based on profiling	20	3	3	3	2	3	1	2.5
Controller - processor relationship	22, 26	3	2	1	2	3	2	2.2
Data Protection by Design and Default	23	2	1	2	3	3	3	2.3
Compliance documentation	28	2	2	3	3	3	3	2.7
Breach notifications DPA and DS	31, 32	1	1	3	2	2	3	2.0
DPIAs	33	2	1	3	2	2	3	2.2
Prior authorisation and consultation	34	1	1	3	3	2	3	2.2
DPOs	35	2	2	3	3	2	2	2.3
Codes of conduct	38	2	2	1	2	1	2	1.7
Certification	39	2	2	1	2	1	2	1.7
Adequacy	41	1	1	1	1	3	2	1.5
BCRs	43	1	1	2	1	1	1	1.2
Derogations	44	2	2	3	2	2	2	2.2
One Stop Shop	55	1	1	2	3	3	2	2.0
Administrative sanctions	79	1	1	3	3	3	3	2.3
Freedom of expression	80	2	2	1	3	2	1	1.8
Health data	81	1	1	1	2	3	3	1.8
Research	83	2	1	1	1	2	3	1.7

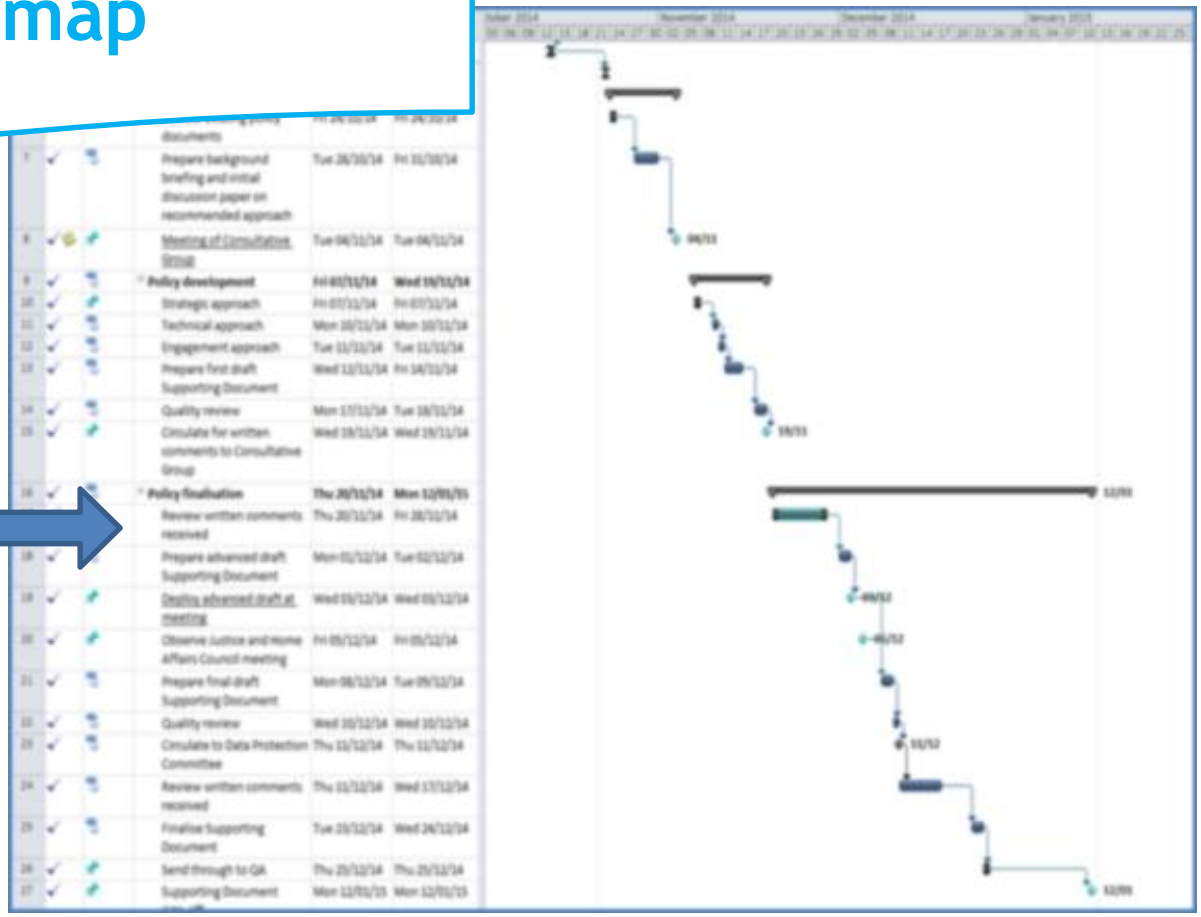
3. Develop custom model

Bespoke impact analysis

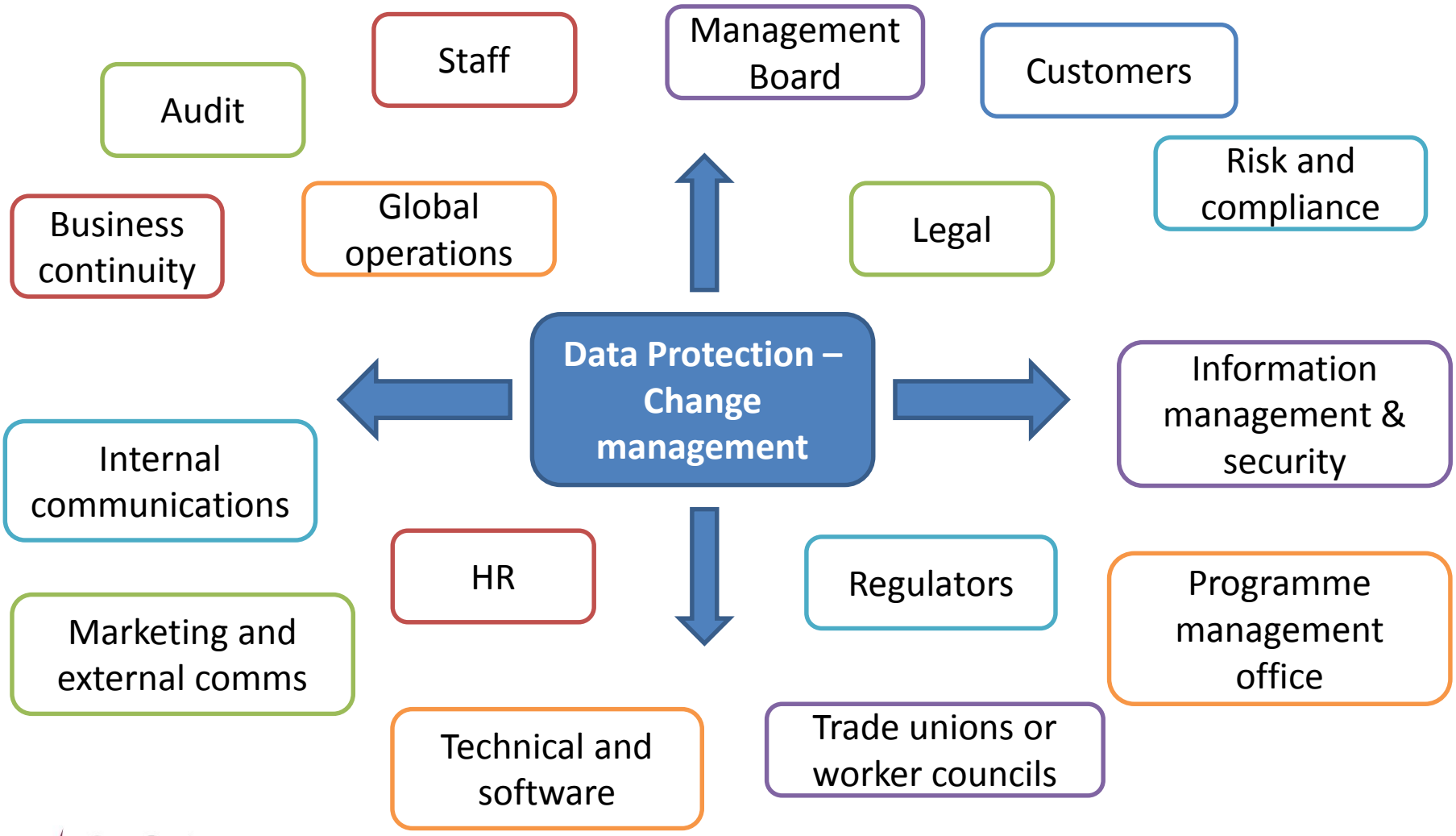


4. Develop change management approach

Transition roadmap



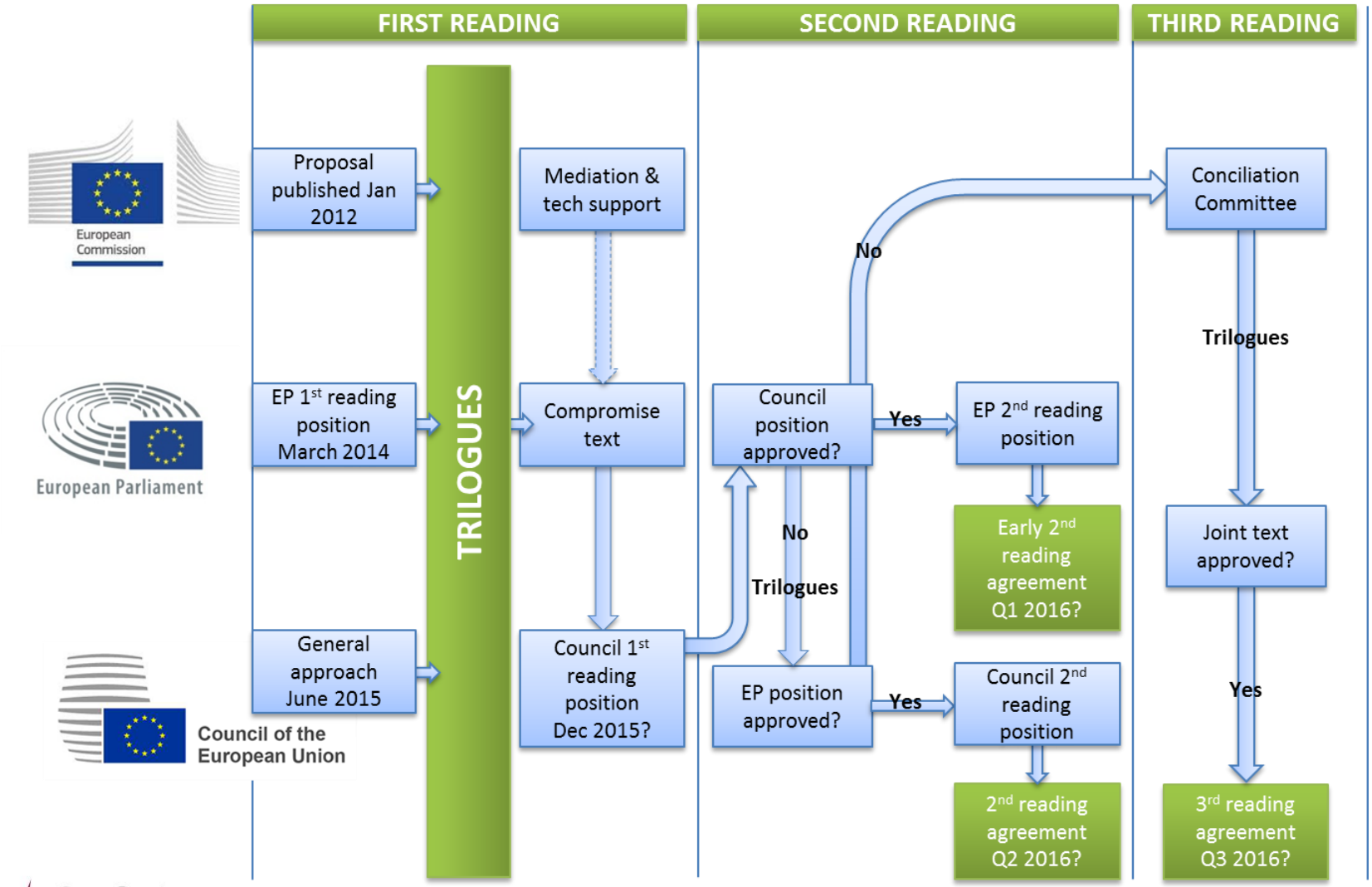
Managing stakeholders and sponsors



The story so far…

“Nothing is agreed until everything is agreed”

Path to agreement



State of play: towards 2015 agreement

"Today we take a big step forward in making Europe fit for the digital age. I am convinced that we can reach a final agreement with the European Parliament and the Council by the end of this year".
Věra Jourová, Commissioner for Justice, Consumers and Gender Equality 15 June 2015

European Commission

eu2015lu.eu
Council of the European Union

"This reform is a package and we have the firm intention to conclude by the end of this year."
Felix Braz, Luxembourg Justice minister 15 June 2015

"We think it's a very good sign that the Council, Commission and Parliament have all committed to agreeing a unified data protection regulation by the end of this year."
Jan Philipp Albrecht MEP, Rapporteur, LIBE Committee 24 June 2015

European Parliament

European Council

"The Data Protection package must be adopted by the end of this year."
European Council conclusions 26 June 2015

Summary: what to do, when to do it

- Appropriate grounds for processing need to be established
- The rights of data subjects will be enhanced and will need to be met
- There will be new obligations on data controllers and processors
- The GDPR is coming, start planning at the earliest opportunity

3. GDPR EXERCISE

Scenario

we-r-board.com

the social network for surfers

1. Global Headquarters in California

2. Marketing offices in 6 EU countries but no designated EU HQ

3. Collects and processes personal data in US and EU and transfers data between the two

4. User personal data has become accessible on a 3rd party website

5.. PII posted includes, names, addresses, location, photos, IM chat feeds, and password prompts

Exercise part 1

What questions do you need to ask?

Exercise part 2

How will the new rules apply?

1. On what grounds will we-r-board.com be able to process and transfer personal data?

2. How will the rights of subjects and obligations on controllers and processors differ between the US and the EU?

3. Complaints about the data breach are being filed across multiple EU jurisdictions. Which DPA is competent?

4. How could the case be resolved?

5. What technical and organisational measures should we-r-board.com take to prepare for the GDPR?

Session objectives

- This session will provide an overview of the key impacts that the GDPR will have on businesses that process the personal data of EU residents
- There will be a focus on what the GDPR means for North American-based data controllers and processors and what businesses can do to prepare for the new rules
- There will be an update on the state of play in GDPR negotiations
- There will be a scenario-based exercise which will highlight key issues that need to be considered in the context of the GDPR
- Delegates should take away an improved understanding of the technical and organizational measures the should adopt in order to be compliant with the GDPR

Questions