

# GDPR compliance workshop



**EU** GDPR  
INSTITUTE

**COPENHAGEN**  
**COMPLIANCE**  
Global GRC Solutions

## GDPR where to start?

# Workshop agenda



- Key impacts of GDPR
- The identification of key deliverables
- Examples from 3 GDPR Implementations
- Descriptions of each deliverable, the key tasks and resources
- Together we develop the roadmap/Framework

# Topic-Input-Process-Output



#	Topic	Input	Process	Expected output
1.	Welcome & introductions	Name, responsibilities, knowledge of data protection	Roundtable presentations	Alignment of workshop participants
2.	GDPR – key impacts and key principles	List of key changes in relation to existing legislation and key principles	Presentation and explanation of each change	Alignment of workshop participants
3.	Presenting the impact analysis model	Process and template	Walkthrough of process and template with examples	Knowledge of how to use the model
4.	Impact analysis group work	Breakout into work groups (Legal, IT, Business, HR, Security); process & templates	Each group identifies and documents impacts against process, organisation/ people, technology & information	1. Cut overview of impacts
5.	Presentation of impacts to workshop	Identified areas per work group	Presentation & feedback	Alignment and updated overview of impacts
6.	Presenting the model for identifying and describing key deliverables	Key deliverable model and template	Walkthrough of model & template with examples	Knowledge of how to use the model
7.	Key deliverables group work	Breakout into work groups; GDPR requirements, key impacts list	Identify key deliverables	1. Cut overview of key deliverables
8.	Describing the key deliverables briefly	Breakout into work groups; Key deliverables list	Briefly describe the key deliverables, identify owners, key tasks	Key deliverable descriptions
9.	Finalising the roadmap – dependencies and timings	List of key deliverables and internal milestones	Develop roadmap by scheduling the key deliverables across a timeline	1. Cut GDPR Roadmap
10.	Next steps and close	GDPR Roadmap	Review of early deliverables and agree key tasks and ownership	Action plan

# Why GDPR is important?

**Fines!**



For less important breaches:

**NEW** 10M EUR up to  
2% global revenue in  
last year

For more important breaches:

**NEW** 20M EUR up to  
4% global revenue in  
last year

Reduced with appropriate technical and organisational measures

# Current data protection dilemma



Multiple platforms, tight budgets,  
impossible schedules, cost overruns.....

# GDPR Components and Goals

- 1 • Key definitions
- 2 • Bands of penalties and range of awards for breaches
- 3 • Timeline to application of GDPR
- 4 • Six data protection principles, lawfulness and consent
- 5 • Sensitive data
- 6 • Rights of data subjects
- 7 • Controllers and processors
- 8 • Data protection by design
- 9 • Securing personal data
- 10 • Reporting data breaches
- 11 • How to perform a DPIA (data protection impact assessment)
- 12 • Role of the DPO (data protection officer)
- 13 • Role of certifications
- 14 • Transferring personal data outside the EU
- 15 • Powers of supervisory authorities
- 16 • Lead supervisory authority
- 17 • Role of the EDPB (European Data Protection Board)

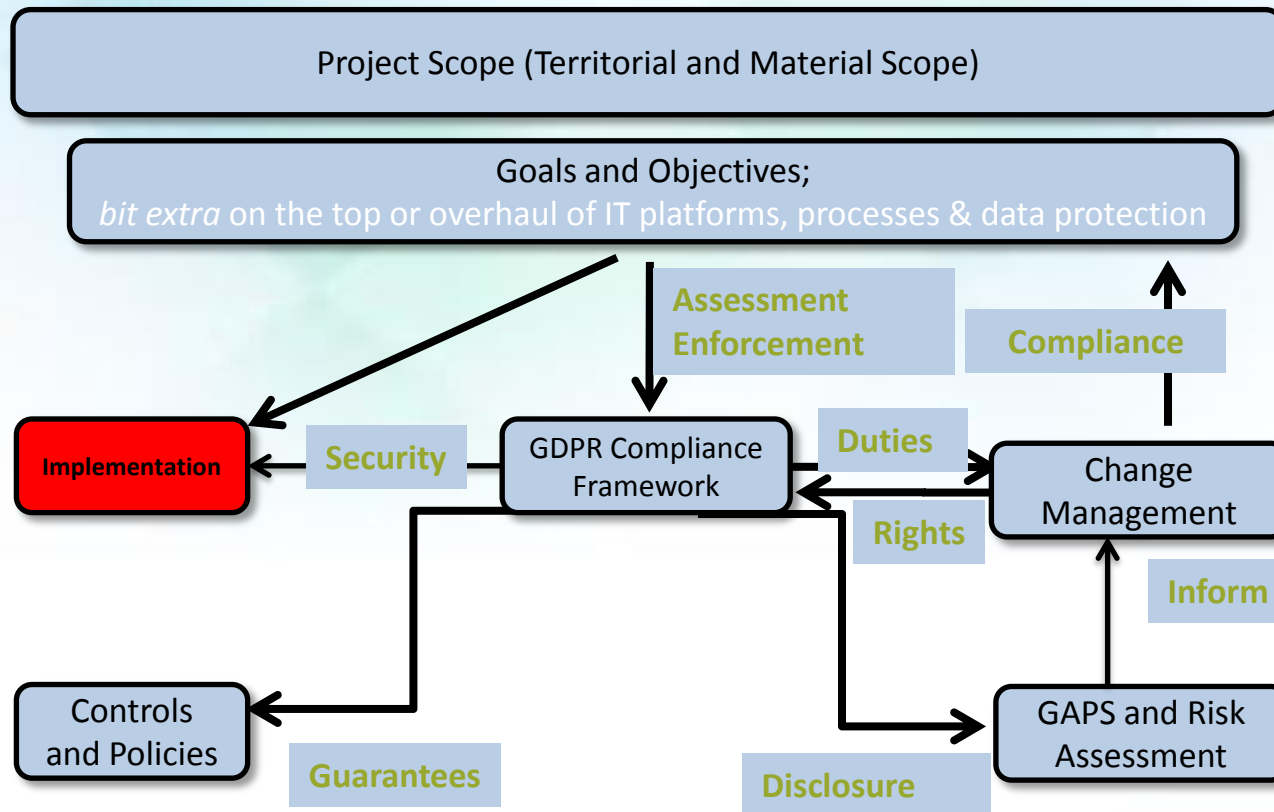
# Recital 10, Brainstorming!



## Processing of personal data, legal obligations for data subjects

- ensure a consistent & high level of protection
- obstacles to personal data flow in the processes
- Concerns on protection, rights and freedom
- Consistency on application to process data
- Margin of flexibility to specify personal data ('sensitive data')

# Key components of a GDPR organisation





# Step I: How can we comply?

## WHAT DO WE NEED TO DO!

- ✎ Organise and control data
- ✎ Remove unnecessary data
- ✎ Streamline the current IT platform
- ✎ Identify privacy vulnerabilities at an early stage
- ✎ Focus client and customer contact lists
- ✎ Privacy is a competitive advantage
- ✎ Protect the companies reputation

# Step 2: How can we comply?



- Existing processes/procedures for adaptation
  - new processes needed
  - new roles and responsibilities, new competencies,
  - training, education, awareness, change of mindset
- Technology e.g. changes to existing applications & infrastructure, new systems, supporting tools during and after the project
- Information assets. e.g. changes to current and formulation of new strategies, policies, contracts, agreements

# Step 3: Clean the house!



The GDPR is an opportunity to improve data and IT practices

De-risk!

- ✎ Stop asking for personal data which is not needed
- ✎ Delete personal data after it is not longer needed
- ✎ Restructure databases to avoid redundancies in personal data
- ✎ Centralize channels to receive personal information


# Step 4: Develop a GDPR center of excellence



- A GDPR technological platform with a dynamic register
  - A platform for learning, guidance & engaging conversations
- Provide solutions to promote integration and compliance
- Response on groundbreaking topics on burning platforms
- Share wisdom of integration, embedding and automating
- Technology modules & solutions to tie tools to platform
  - Templates, checklists, assessment tools, thought leadership
  - webinars, access to experts, guidance, connect & online tools
- Stay one-step ahead of the authorities with benchmarks.

# Group discussion







 **Which department(s) hold most of the personal data in your organisation?**



# Step 1: Compile a data inventory



-  **What personal data do we hold?**
-  **Where is it?**
-  **What is it being used for?**
-  **How secure is it?**

# Step 2: Compile a data inventory



## Who

- are the data subjects?
- has access to their personal data?

## Where

- the personal data is stored?
- the personal data is transferred?

## Why

- the personal data is under the company control?

## When

- the personal data is kept until?
- Is shared with third-parties?

## What

- safety mechanisms and controls are is placed  
Does the Law and the mandates says?

# Step 3: A bad example

INDUSTRY NEWS > MANUFACTURING

## Boeing discloses 36,000-employee data breach after email to spouse for help

Feb 28, 2017, 5:52pm PST Updated Mar 1, 2017, 9:16am PST

Think twice before asking your spouse for help formatting a document, especially if it contains personal information for 36,000 of your co-workers.

Boeing launched an internal security investigation and notified Washington state Attorney General [Bob Ferguson](#) and officials in California, North Carolina and Massachusetts that employee data left control of the company when a worker emailed a spreadsheet to his significant other.

Boeing said the unnamed employee told investigators he sent the document to get his spouse's help on some formatting issues.



# Step 4: Impact Assessment

NEW

COPENHAGEN  
COMPLIANCE

- Describe the processing
- Assess the need and the proportionality of processing
- Assess the risk
- Address the risks


# Step 5: Implement a privacy policy



**Any company in the World has, at least, one employee who would sell private information...  
.... and another one who would click on everything**

# Group discussion

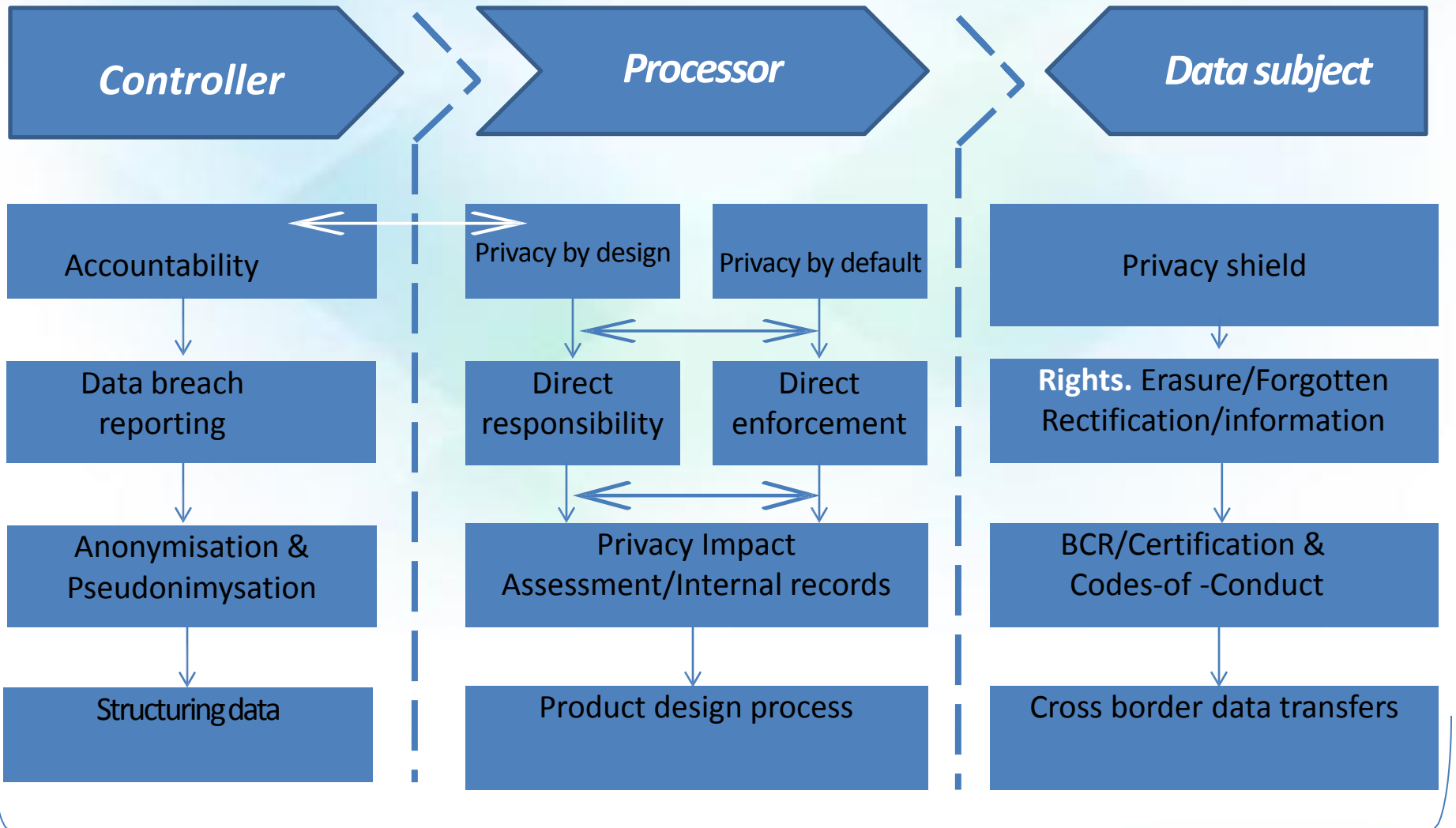


 **How would you link the dataflow map with the cross-border transfers?**



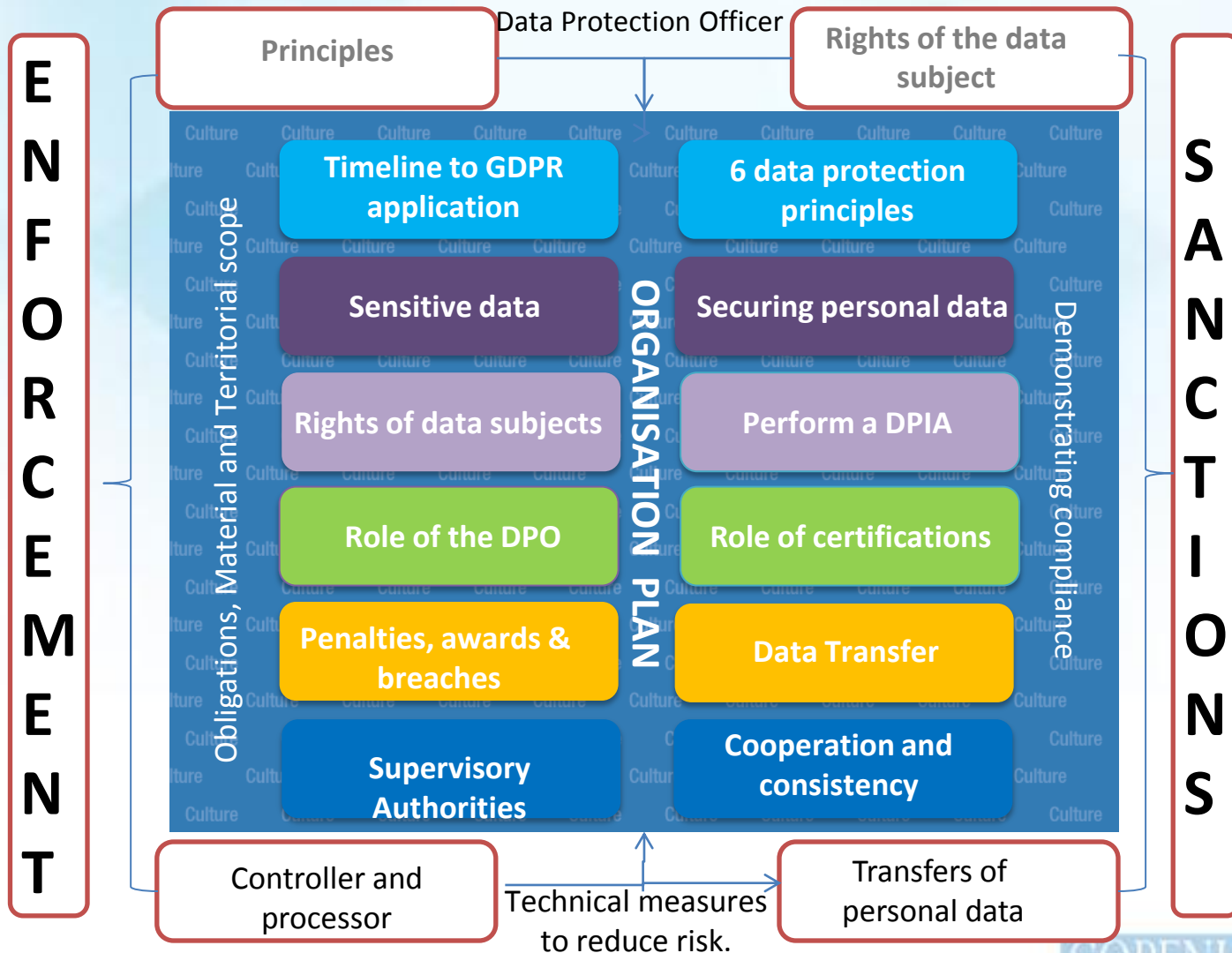
# THE GDPR ROADMAP AND FRAMEWORK

# Assemble the GDPR Road Map & Framework



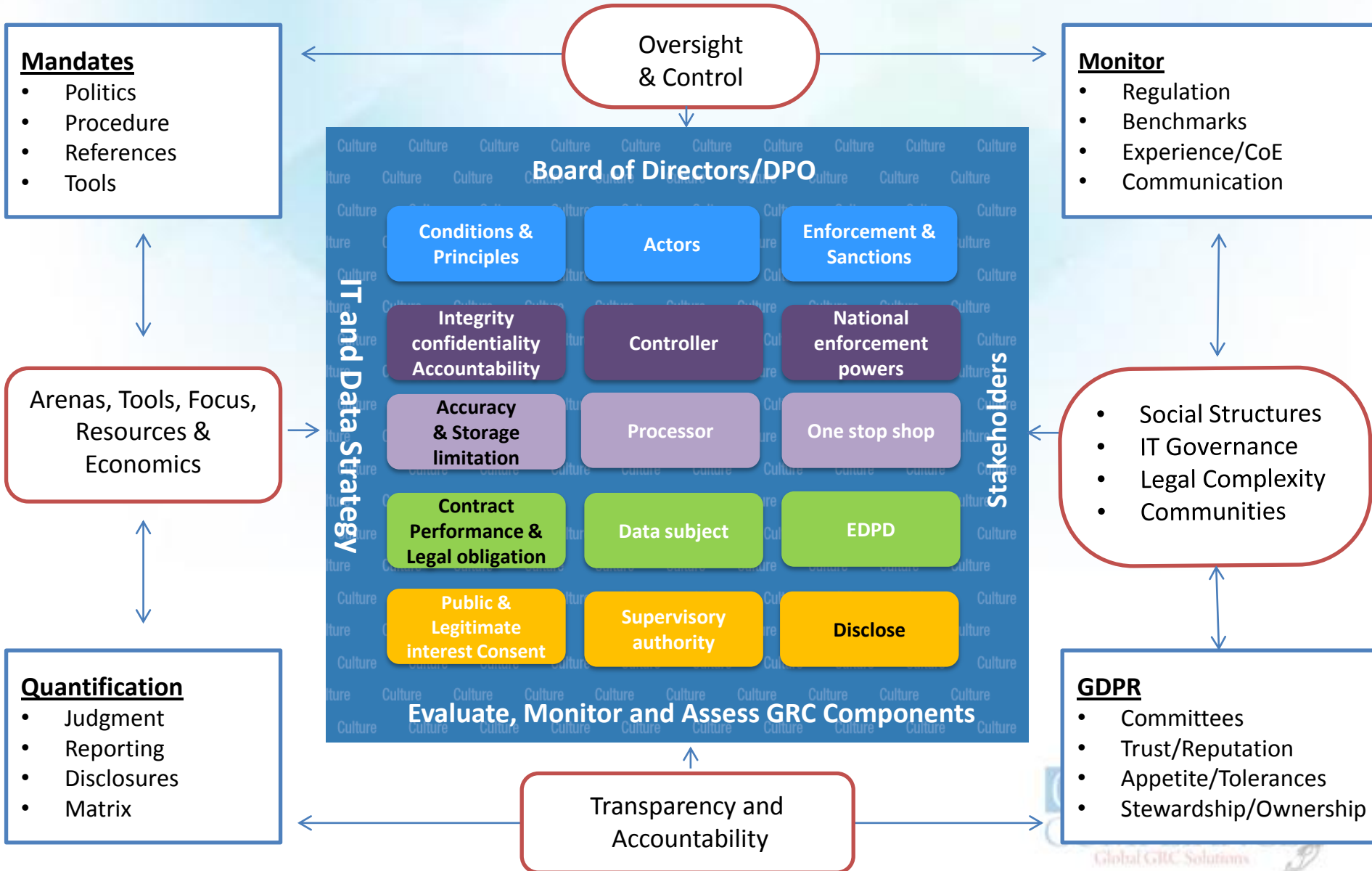
GDPR ROAD MAP & FRAMEWORK

# The GDPR Roadmap



The Roadmap is accompanied by a detailed narrative for measuring, monitoring, disclosures and automation

# Framework to Address GDPR Exposure



The Framework is accompanied by a detailed narrative to measure, monitor and automate data privacy issues

# What's next?

- The EUGDPR Institute
  - Think Tank, Advisory, Conferences, Seminars  
Workshops.
- Further assessments, workshops/training?
- GDPR IT Tool and bespoke review?



Be ready...

COPENHAGEN  
COMPLIANCE

**25 May 2018**

COPENHAGEN  
COMPLIANCE  
Global GRC Solutions 



Kersi F. Porbunderwalla is the Secretary General of Copenhagen Compliance and Managing Partner of Copenhagen Charter and Riskability IT Tools. Kersi is a global consultant, teacher, instructor, researcher, commentator and practitioner on good Governance, Risk Management, Compliance and IT-security (GRC), Bribery, Fraud and anti-Corruption (BFC) and Corporate Social Responsibility (GDPR) issues. Kersi lectures at The Govt. Law College (Thrissur, India) Georgetown University (Washington) and at Fordham University (New York). Kersi has conducted several hundred workshops, seminars and international speaking assignments on Regulatory Compliance, GRC, GDPR, and BFC issues.

**Disclaimer:** This presentation is prepared for EUGDPR Institute GDPR workshop. The content together with the links to narratives, brochures and information on our websites, is for general informational purposes only. Please refer to Copenhagen Compliance® for specific advice on regulatory compliance and other GRC issues.

**Copenhagen Compliance UK Ltd®**

[Info@copenhagencompliance.com](mailto:Info@copenhagencompliance.com)

[www.copenhagencompliance.com](http://www.copenhagencompliance.com)

21, Cloudseley Street, London N1 OHX, UK.

Tel. +44 7778 917 133

Kersi Porbunderwalla tel: +45 2121 0616