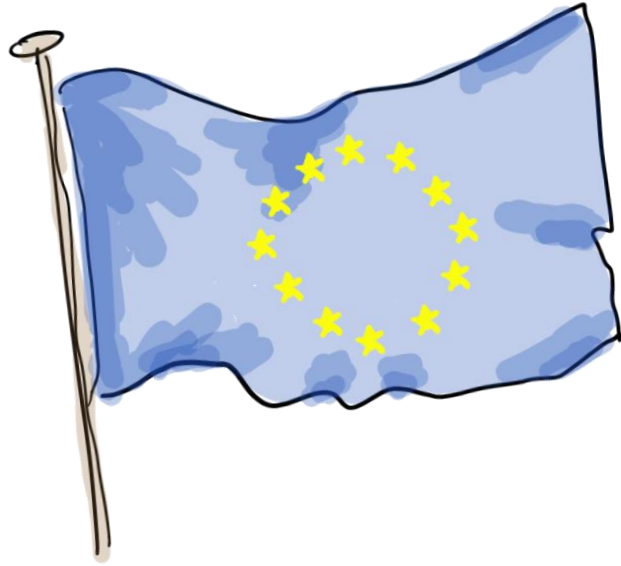


# New European Union Data Privacy Laws Could Cost Your Company Money

*Tim Clements*

Wednesday, 6 December 2017



# Learning objectives

- Assess your organizations current state of data collection management
- Recognize customer personal data and identify where and how it is collected, created, stored, used, transferred and eliminated
- Identify the key deliverables including policies and procedures that your enterprise needs to comply with the GDPR

# Agenda

- Introduction to the General Data Protection Regulation (GDPR)
- Pinpointing personal data
- Purposes of processing
- Assessment tools
- Data flow mapping
- Identifying project scope
- A slide for busy executives

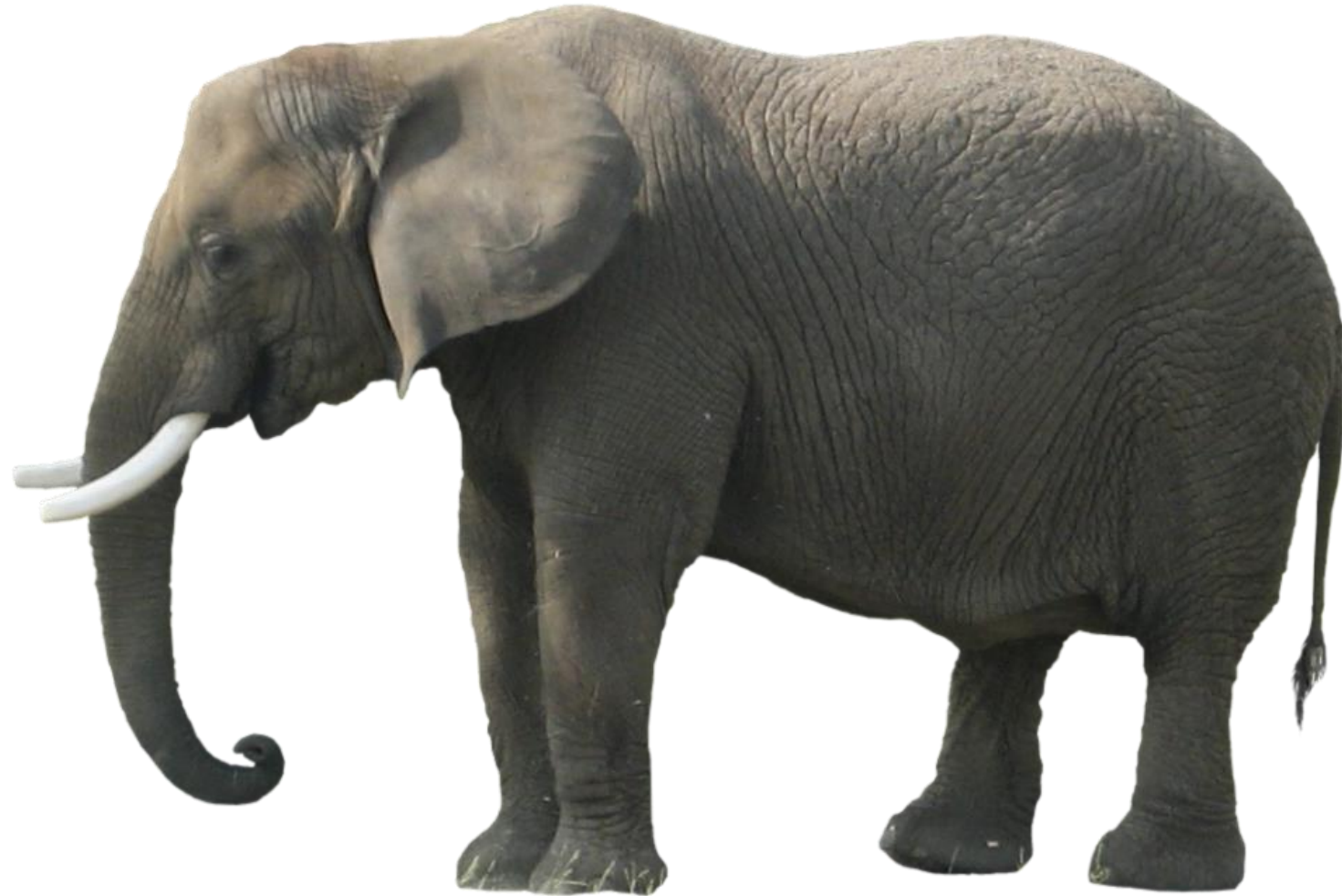
# Introduction



# GDPR - the scale of the challenge

“When eating an elephant  
take one bite at a time”

*Creighton W. Abrams*

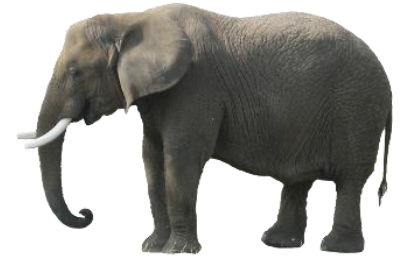


# The scale of your challenge?



*How compliant are you with existing  
data protection legislation?*

*...and are you able to demonstrate it?*

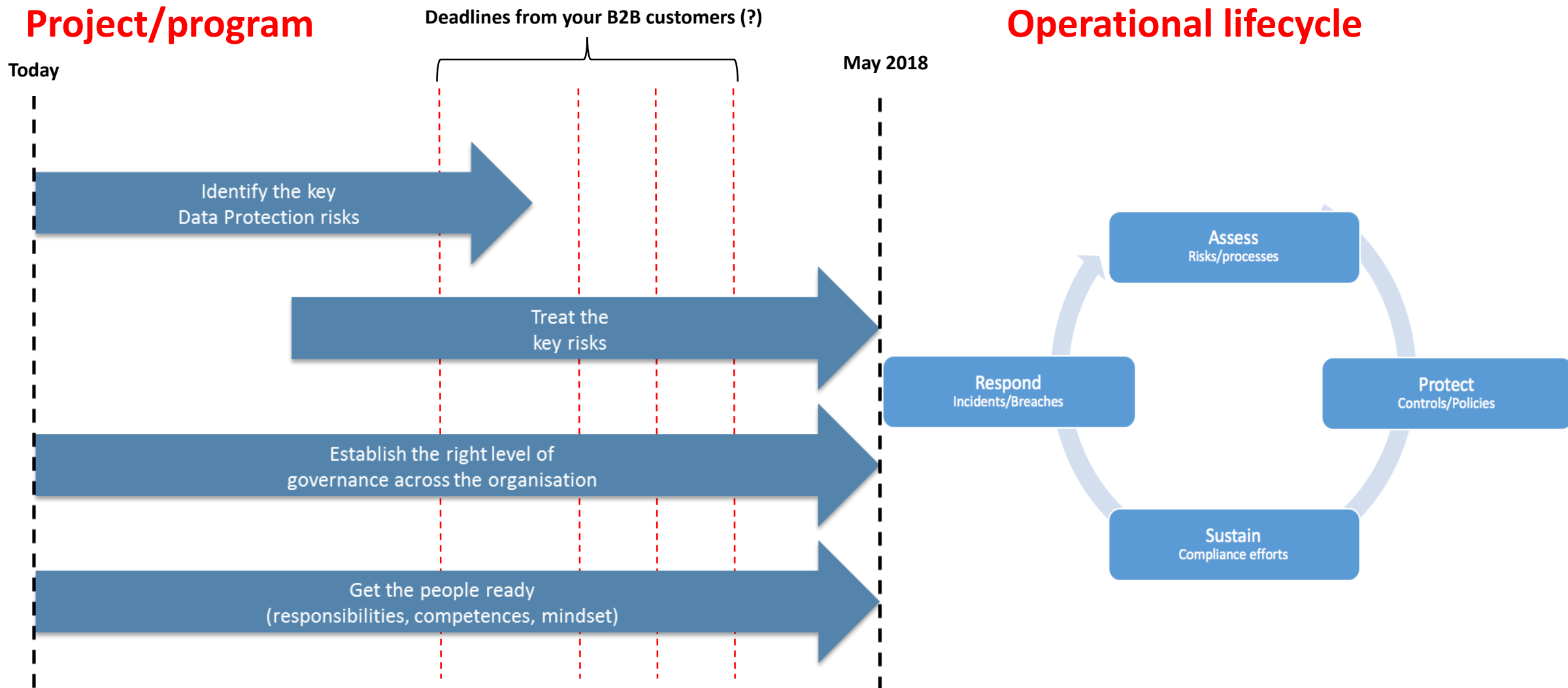


*GDPR – a “bit extra” on top of an existing regime*



*GDPR – a new recipe may be needed*

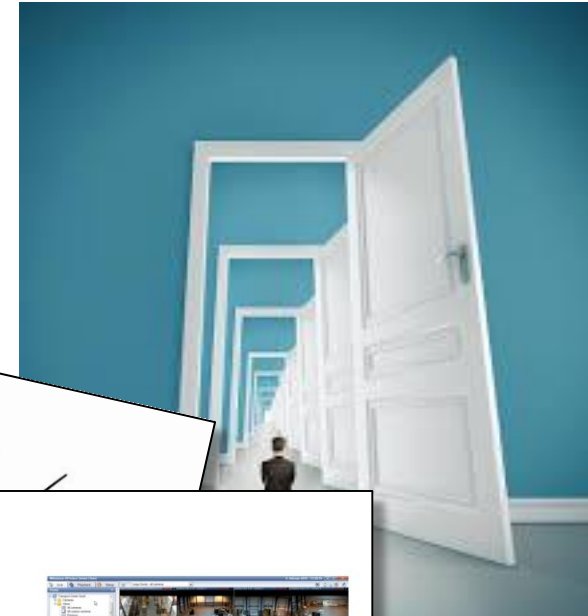
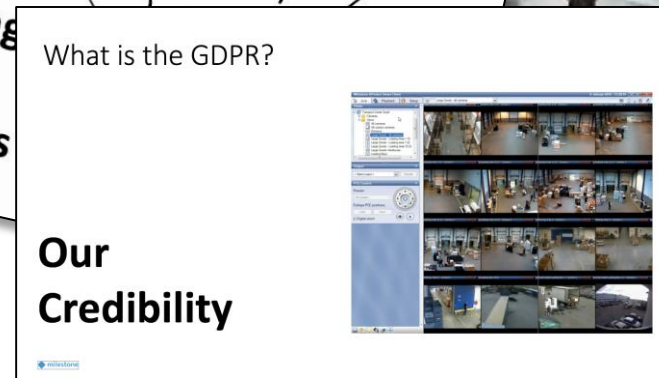
# GDPR – just another compliance project/program?



# How are you framing your GDPR challenge?



**Barrier**



**Opportunities**



# High level view of the GDPR

## What organizations have to do



Keep records of all processing of personal information



Institute safeguards for cross-border data transfers



Maintain appropriate data security



Collect personal data lawfully and fairly, and where relevant, get appropriate consent and provide notification of personal data processing activities



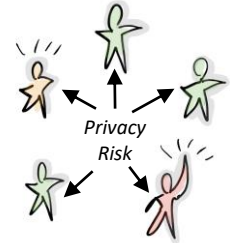
Get a parent's consent to collect data for children under 16



Consult with regulators before certain processing activities



Provide appropriate data protection training to personnel having permanent or regular access to personal data



Conduct Data Protection Impact Assessments on new processing activities



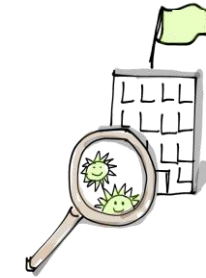
Implement Data Protection-by-Design (*Privacy "baked-in"*)



Take responsibility for the security and processing activities of third-party vendors



Appoint a Data Protection Officer (if you regularly process lots of data, or particularly sensitive data)



Be able to demonstrate compliance on demand



Notify data protection agencies and affected individuals of data breaches in certain circumstances

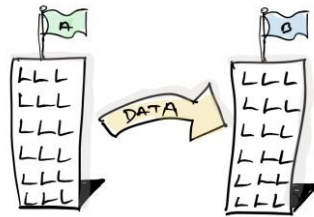
## What individuals can do



Withdraw consent for processing



Request a copy of all of their data & request corrections if wrong



Request the ability to move their data to a different organization

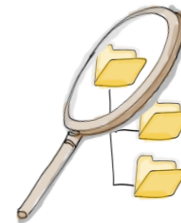


Request that their information is deleted when there's no purpose to retain it

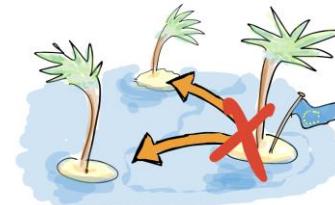


Object to automated decision-making processes, including profiling

## What regulators can do



Ask for records of processing activities and proof of steps taken to comply with the GDPR



Suspend cross-border data flows

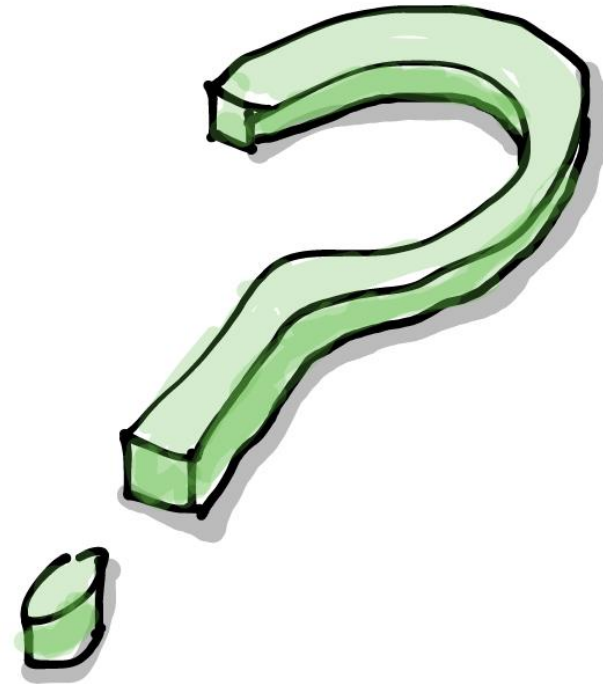


Impose temporary data processing bans, require data breach notification, or order erasure of personal data

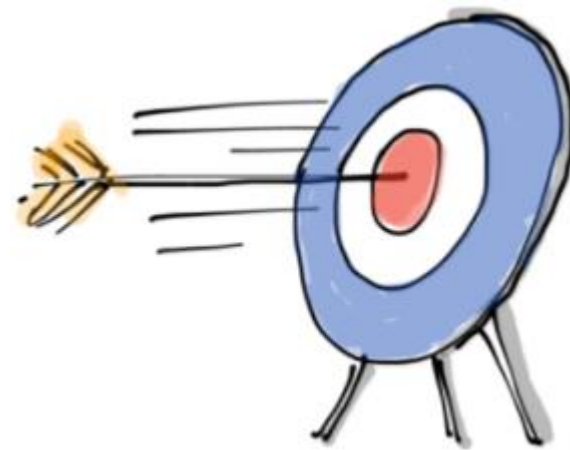


Enforce penalties of up to €20 million or 4% of annual revenues for non-compliance

Remember to  
submit questions via  
the Q&A function



Pinpointing  
personal data



# Categories of personal data

Categories of personal data	Sensitive personal data
-----------------------------	-------------------------

Information about economic and financial aspects (salary, financial situation, fiscal situation, etc.)

Data related to health

Personal life (habits, family situations, etc.)

Data revealing racial or ethnic origin

Biometric data intended to identify an individual physical person

Civil status, identity, identifiable information, images, etc

Connection details (IP address, log files, etc.)

Data related to sex life or orientation

Data related to criminal convictions or offences

Localisation details (movements, GPS coordinates, GSM, etc.)

National identification number

Data revealing union membership

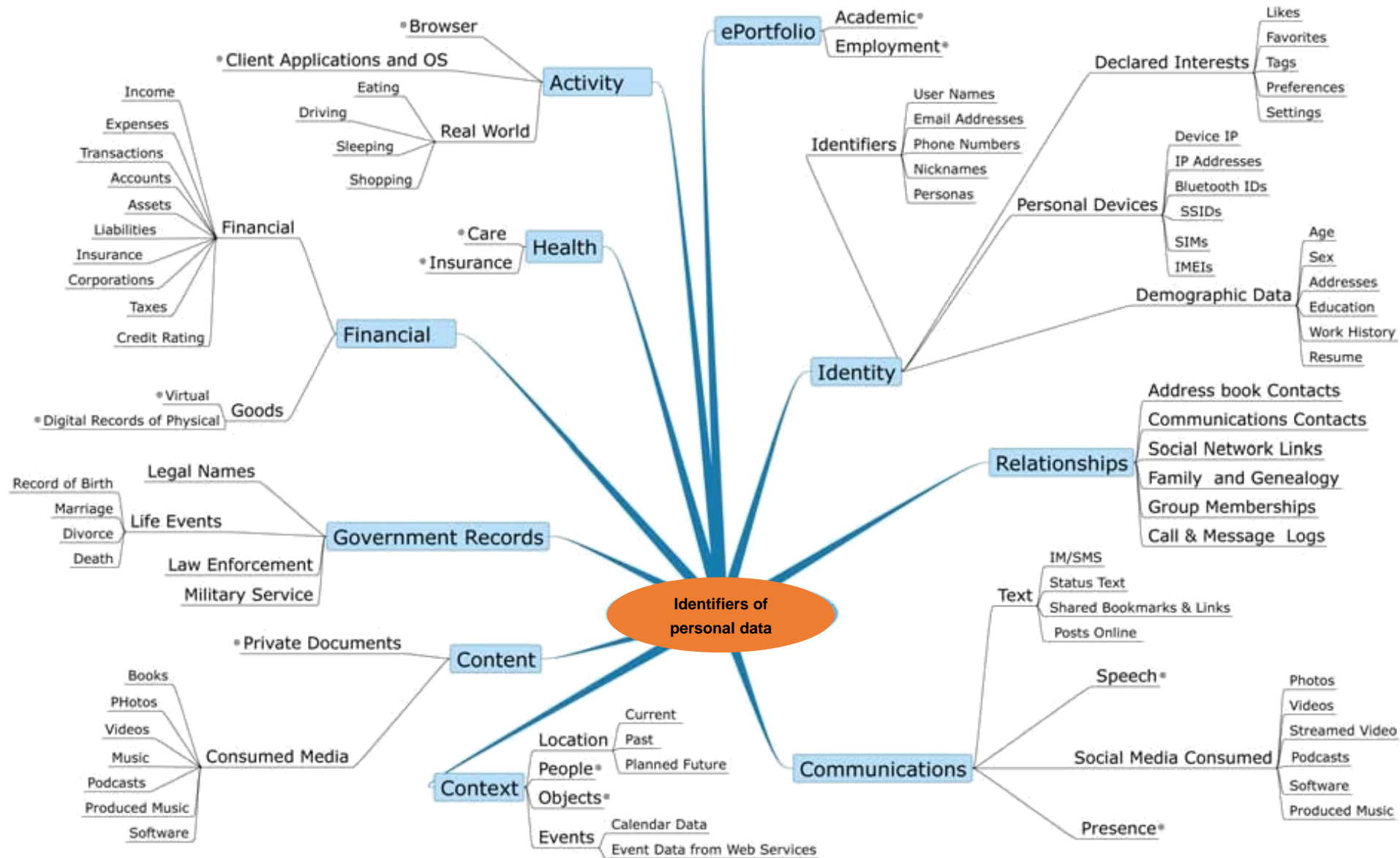
Data revealing religious or philosophical beliefs

Genetic data

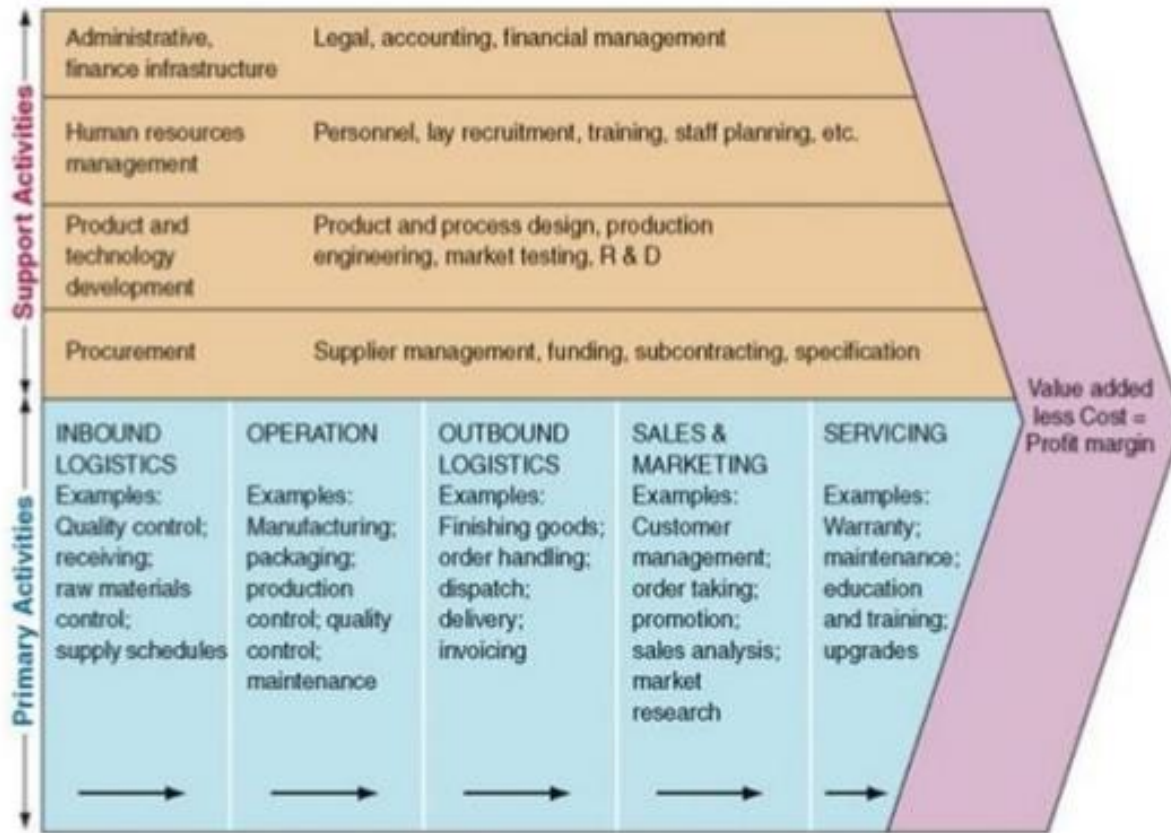
Data revealing political opinions



# Examples of Personal data identifiers



# Starting Point - Value Chain Map



The idea of the value chain is based on the process view of organisations, the idea of seeing a manufacturing (or service) organisation as a system, made up of subsystems each with inputs, transformation processes and outputs.


*In the GDPR Project, the Value Chain Map provides a useful context of identifying data flows containing personal data.*



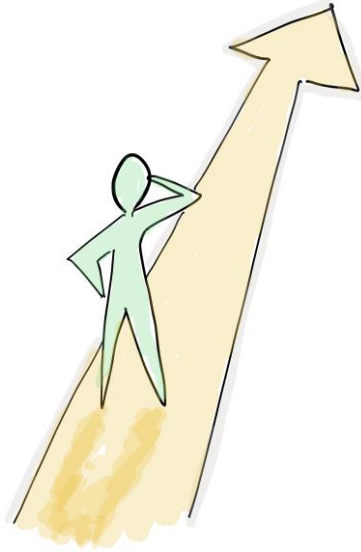
# Overview of processes

## - Generic HR example

HR Services											
HR Strategy & Planning 1.0	Organisational Development 2.0	Recruitment 3.0	Employee Management 4.0	Payroll & Benefits 5.0	Time & Attendance 6.0	Learning Management 7.0	Performance Management 8.0	Talent Management 9.0	Health and Safety 10.0	HR Information 11.0	HR Function 12.0
Analyse trends & requirements 1.1	Define org. Values & Objectives 2.1	Develop & Maintain Recruitment Policies 3.1	Develop & Maintain Personnel Policies 4.1	Develop & Maintain Salary & Benefits Packages 5.1	Resource Planning & Budgeting 6.1	Develop & Maintain Learning Policies 7.1	Develop & Maintain Performance Policies 8.1	Develop & Maintain Talent Policies 9.1	Develop & Maintain H&S Policies 10.1	Develop & Maintain HR Data Policies 11.1	Manage HR Resources 12.1
Create HR Strategy 1.2	Define org. Models & Structures 2.2	Produce Recruitment Plans 3.2	Data Management & Maintenance 4.2	Payroll Administration 5.2	Time Management 6.2	Assess & Plan Development Needs 7.2	Manage Probations & Trials 8.2	Manage Org. Reviews 9.2	Provide H&S Advice 10.2	Administer HR Data Changes 11.2	Develop & Maintain HR System 12.2
Create Business Unit People Strategies 1.3	Create Job Descriptions 2.3	Manage Authorisation Process 3.3	Organisational Structure recording 4.3	Benefits Administration 5.3	Record & Manage Absence 6.3	Plan & Schedule Learning Sessions 7.3	Manage Perf. & Potential Reviews 8.3	Develop & Maintain TD Programme 9.3	Conduct H&S Audits 10.3	Provide HR KPI Reporting 11.3	HR Line Mgt. 12.3
Create HR Development Plans 1.4	Evaluate Jobs 2.4	Design Recruitment Campaign 3.4	Contact information sites 4.4	Pension Administration 5.4	Temporary Leave 6.4	Develop & Maintain Training Materials 7.4	Manage 360 degree survey 8.4	Manage Succession Planning 9.4	Manage H&S Reporting 10.4	Manage HR Data Integrity 11.4	Manage HR Perform. 12.4
Create HR Financial Plans 1.5	Administer Template Changes 2.5	Candidate Management 3.5	Employee Records 4.5	Travel & Expenses Administration 5.5	Compensation Management 6.5	Deliver Learning Sessions 7.5	Manage Employee Engagement Survey 8.5	Record Talent Development Results 9.5	Manage H&S Incidents 10.5	Manage Call Handling 11.5	Manage Internal Suppliers 12.5
	Manage External OD Suppliers 2.6	Pre-screening & Assessment 3.6	Employee Movements 4.6	Payroll Accounting 5.6	Negotiate Union Agreements 6.6	Evaluate Learning Effectiveness 7.6	Record Perf. Management Results 8.6	Manage External T&D Suppliers 9.6	Manage External H&S Suppliers 10.6		Manage HR Projects 12.6
		Interview & Selection 3.7	Employee Case Handling 4.7	Bonus Administration 5.7	Administer Union Agreements 6.7	Competence Documentation & Reporting 7.7	Manage External Perf. Mgm. Suppliers 8.7				
		New Joiner Handling 3.8	Relocation Administration 4.8	Termination Benefits 5.8		Manage External T&D Suppliers 7.8					
		Onboarding Programme 3.9	Exit Handling 4.9	Year-End Processing 5.9							
				Manage External P&B suppliers 5.9							

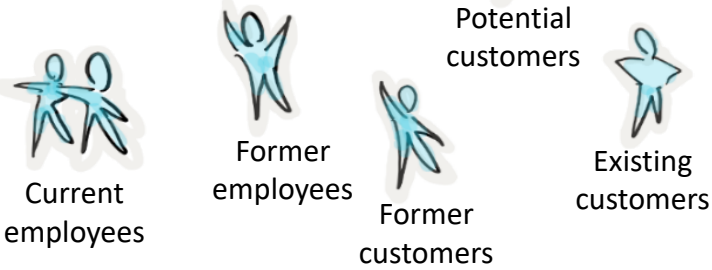
 = in scope

Purposes of  
processing





**DATA SUBJECTS  
(examples)**



**PURPOSES  
(examples)**

"Make a purchase from our online bookshop"

"Personalise the way web content is presented and ensure content from the web site is presented in the most effective manner for you and for your computer"

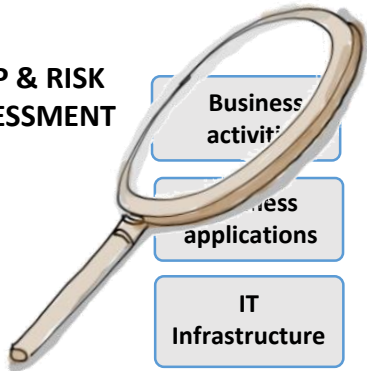
**DATA ITEMS  
(examples)**

Income

Name Address Phone#

DoB ip address

**GAP & RISK  
ASSESSMENT**



**INVENTORY  
OF PROCESSING  
ACTIVITIES**

**LAWFULNESS OF PROCESSING**

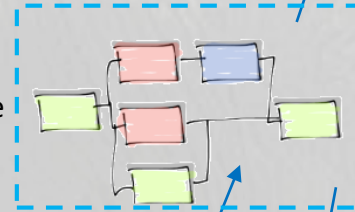
**ROLE**



**PROCESSING ACTIVITY** e.g. "online book purchase"

**DATA FLOW B**  
**DATA FLOW A**

**Data usage**



Disclosure

**Data store**

Deletion

Purpose C

**REPURPOSE (example)**

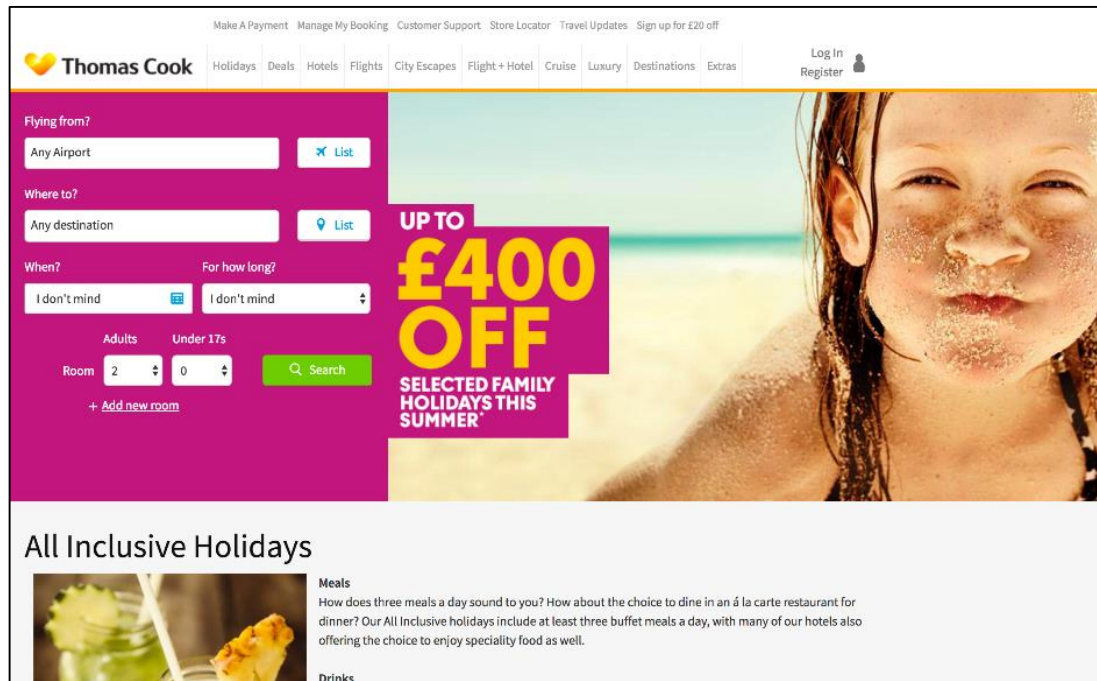
"Report aggregate information to our advertisers"

This elephant belongs to...



Clean up

# Example “purposes” – travel company (website)



The screenshot shows the Thomas Cook website interface. At the top, there is a navigation bar with links: Make A Payment, Manage My Booking, Customer Support, Store Locator, Travel Updates, Sign up for £20 off, Log In, and Register. Below this is a secondary navigation bar with categories: Holidays, Deals, Hotels, Flights, City Escapes, Flight + Hotel, Cruise, Luxury, Destinations, and Extras. The main content area features a large booking form on the left with fields for 'Flying from?' (Any Airport), 'Where to?' (Any destination), 'When?' (I don't mind), and 'For how long?' (I don't mind). It also includes dropdowns for 'Adults' (2) and 'Under 17s' (0), a 'Room' dropdown (2), and a 'Search' button. A '+ Add new room' link is also present. To the right of the form is a large promotional banner for 'UP TO £400 OFF SELECTED FAMILY HOLIDAYS THIS SUMMER' featuring a photo of a child. Below the form, there is a section titled 'All Inclusive Holidays' with a sub-section 'Meals' containing text about dining options and a 'Drinks' sub-section.

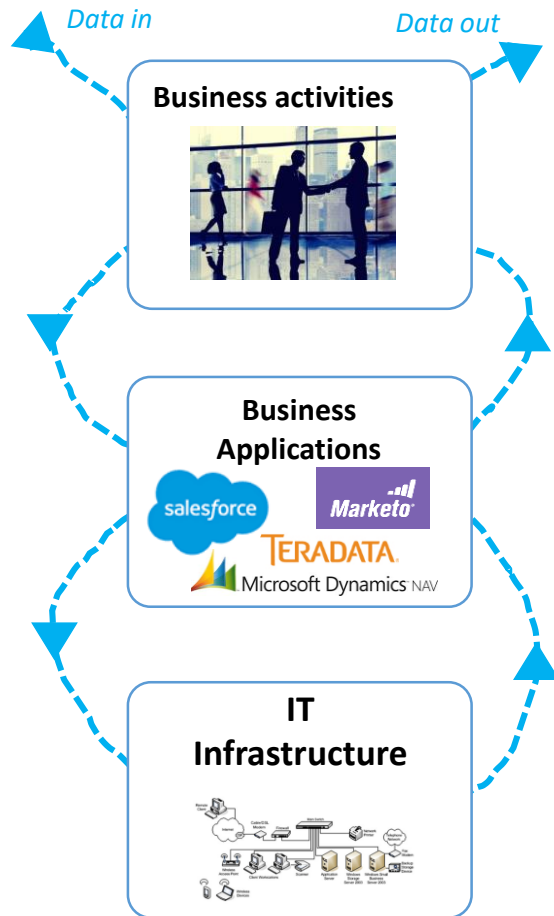
- To make a travel booking
- Enter a competition or promotion
- Complete a survey
- Report a problem with the web site
- Details of transactions carried out through the site and of the fulfilment of bookings/purchases
- Internal research purposes
- Improve customer service
- Report aggregate information to advertisers

## Example “purposes” – employee data



- To assess an individual's qualifications and suitability for a position
- To administer a range of HR processes (e.g. performance review, disciplinary action)
- For remuneration, payroll and pension admin.
- To establish a contact point in the event of an emergency at work
- To manage an employee's interactions with the various facilities and services offered by the organisation (e.g. physical access)
- To establish an employee's training and development requirements

# Simple 3-layer organizational model



## Business activity layer

- Business processes, procedures, activities, work, “getting stuff done”
- These are either automated, manual or a combination of the two
- In-house or 3rd party, or combinations

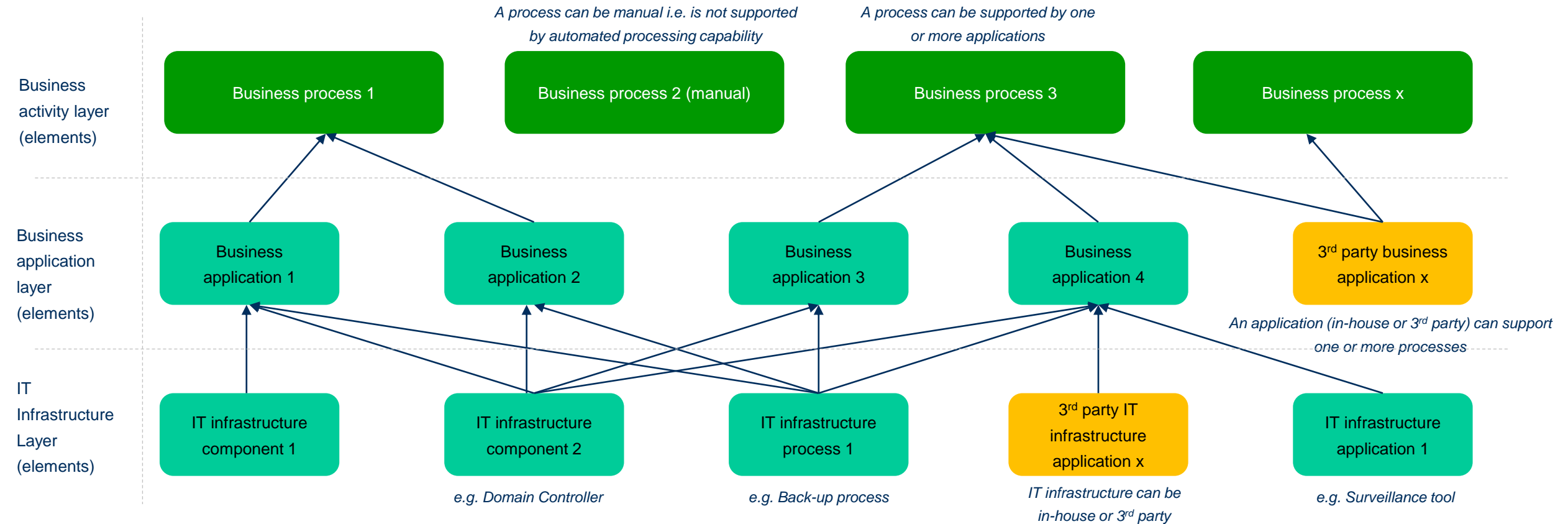
## Business application layer

- Software, applications that provide automated processing to support business activities
- In-house or 3rd party, or combinations

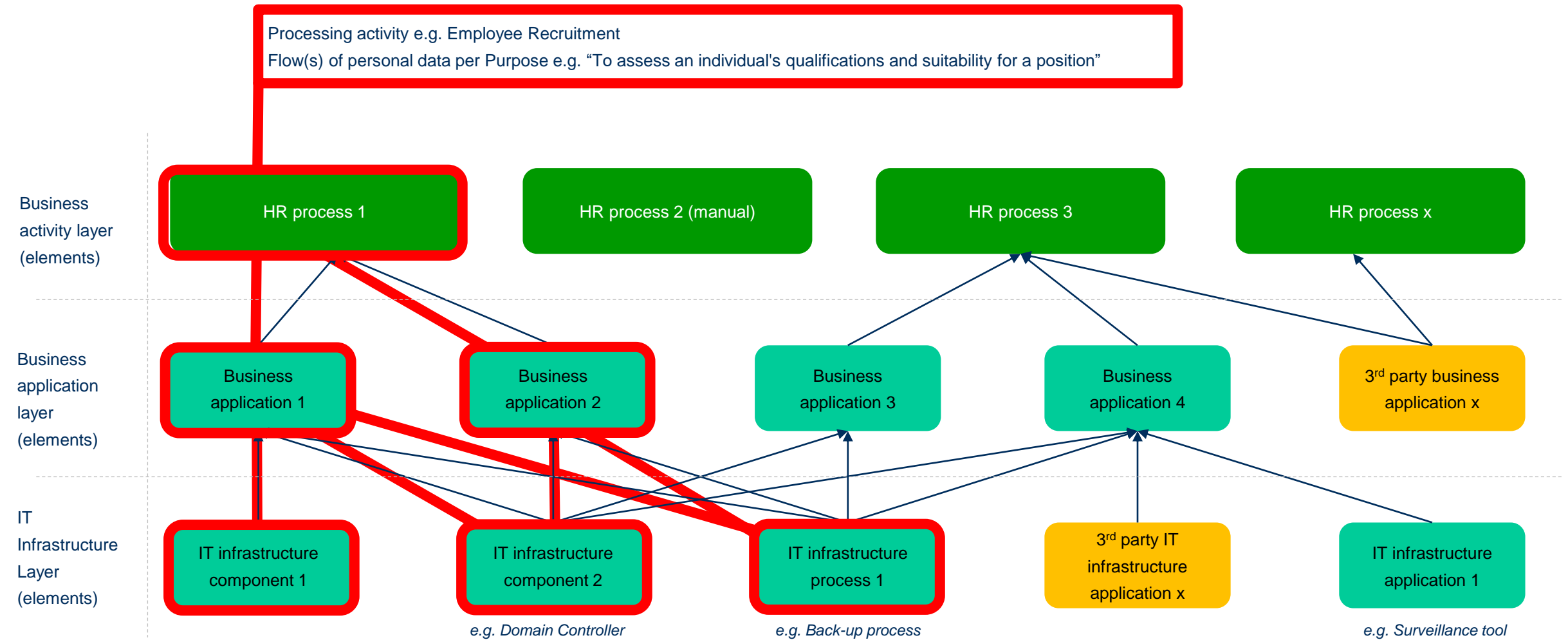
## IT infrastructure layer

- IT processes, hardware components, IT applications, IT services
- In-house or 3rd party, or combinations.

# Identifying data flow scope (conceptual)

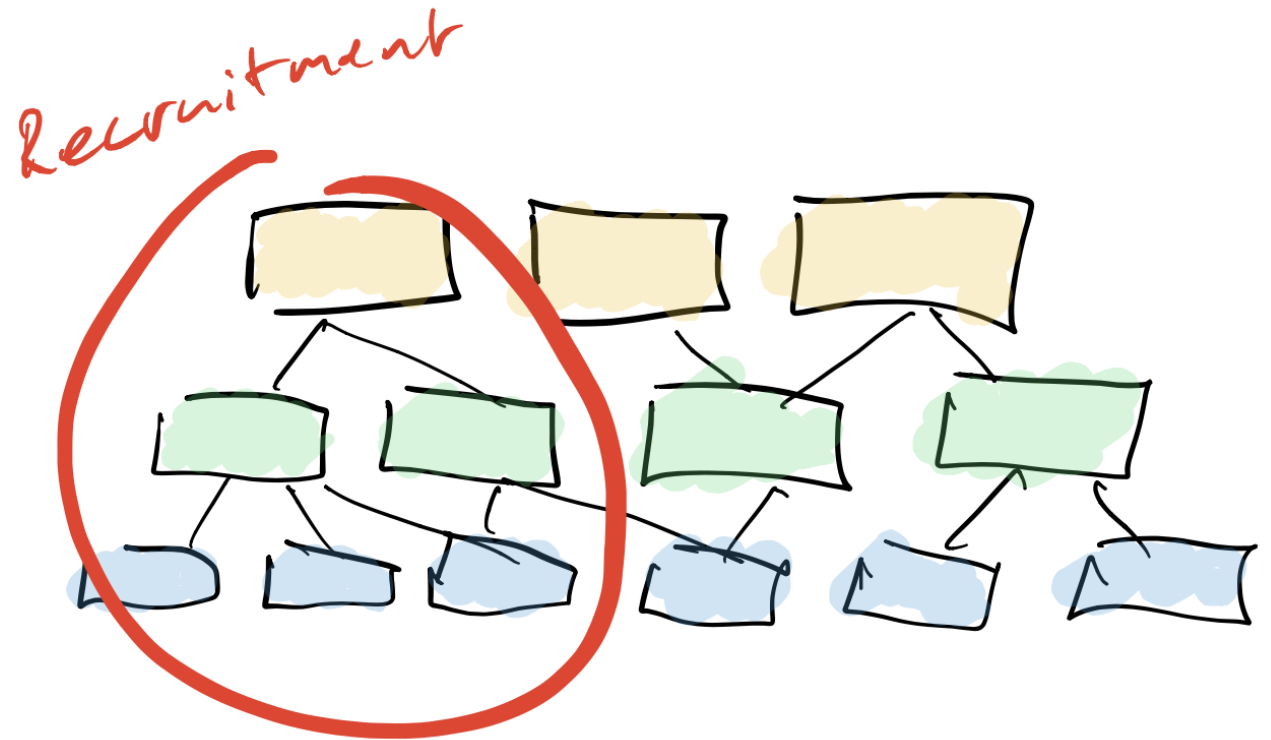


# Identifying data flow scope (conceptual)



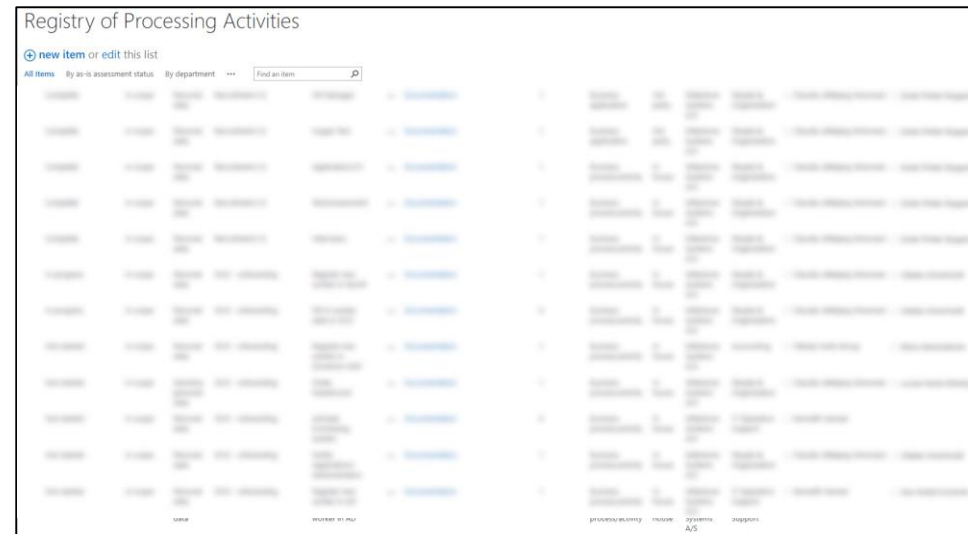


# Assessment tools



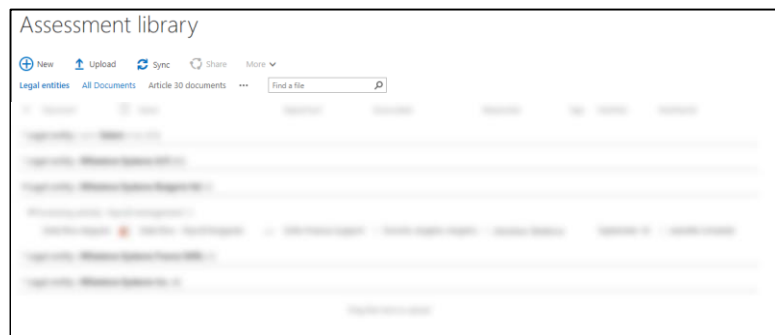
# Internal tools to support Article 30 (Records of processing Activities)

## Registry of processing activities (SharePoint list)



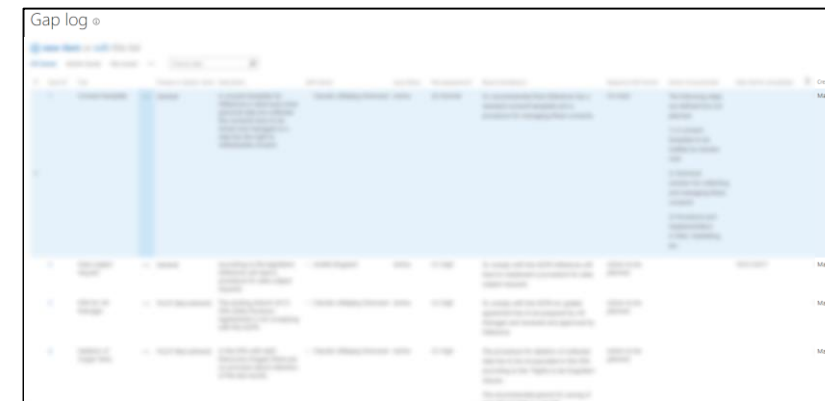
- Processing activity
- Purpose
- Element category (bus. activity, bus. application, IT infra.)
- Element name
- Data type (personal, sensitive, non-personal)
- GDPR scope (in/out)
- Prioritization (e.g. volume, risk, business impact)
- Source (Internal, 3<sup>rd</sup> parties)
- Legal entity
- Department
- Accountable
- Responsible
- Documentation link

## Documentation (SharePoint document library)



Links

## Gap & risk log (SharePoint list)



- Data Flow Diagrams
- Article 30 documents
- Information Security Assessments
- Legal Assessments
- System landscapes
- Assessment reports



# Tool inspiration



## Tool categories:

Activity Monitoring

Assessment Management

Consent Management

Data Discovery

Data Mapping

De-identification/ Pseudonymity

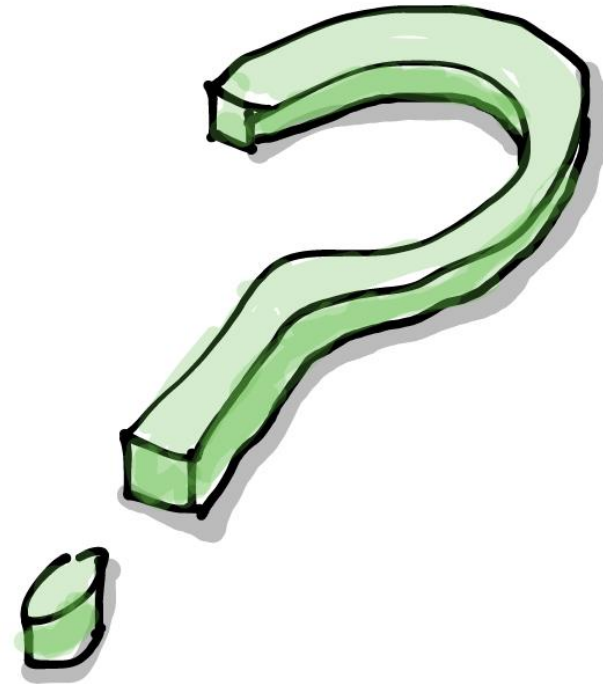
Enterprise Communications

Incident Response

Website Scanning

[https://iapp.org/media/pdf/resource\\_center/Tech-Vendor-Directory-1.4-electronic.pdf](https://iapp.org/media/pdf/resource_center/Tech-Vendor-Directory-1.4-electronic.pdf)

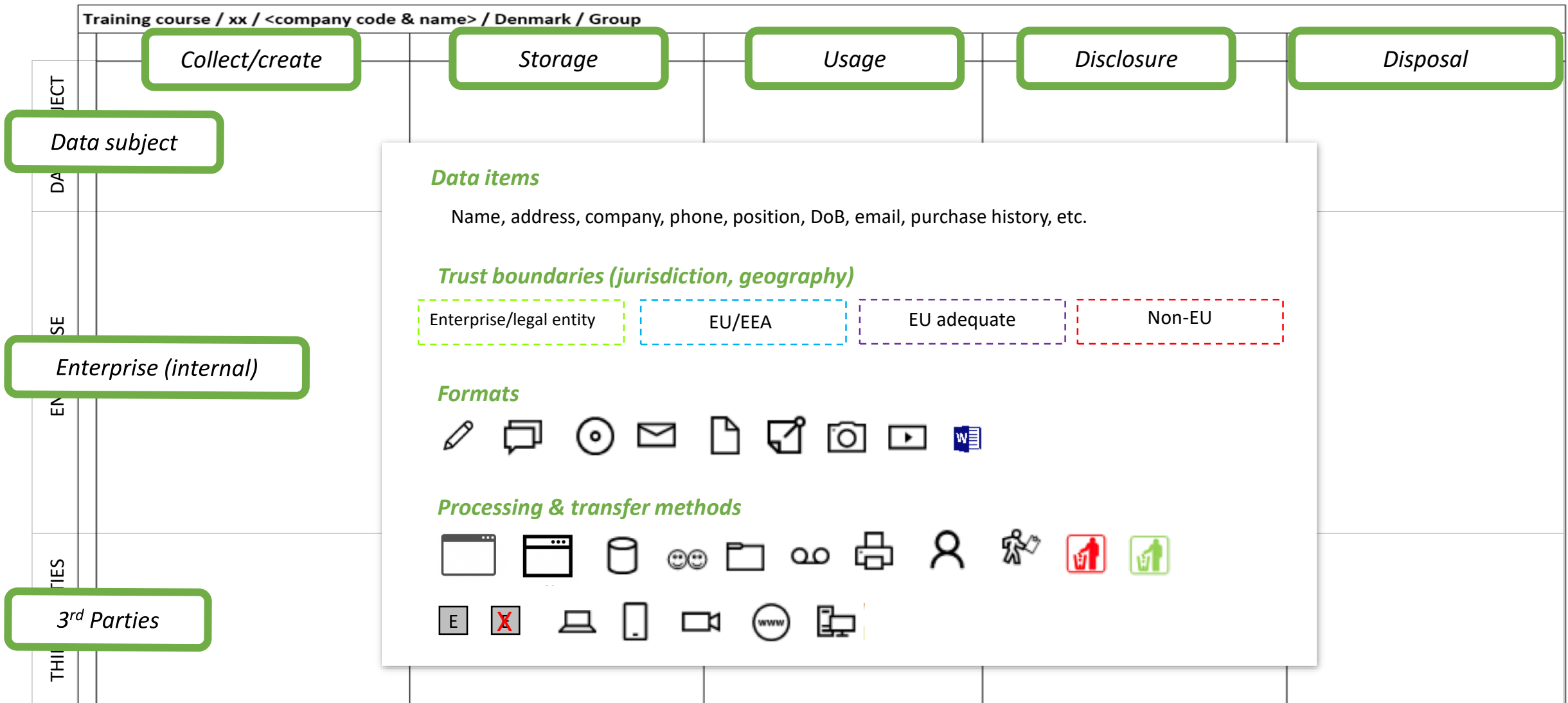
Remember to  
submit questions via  
the Q&A function



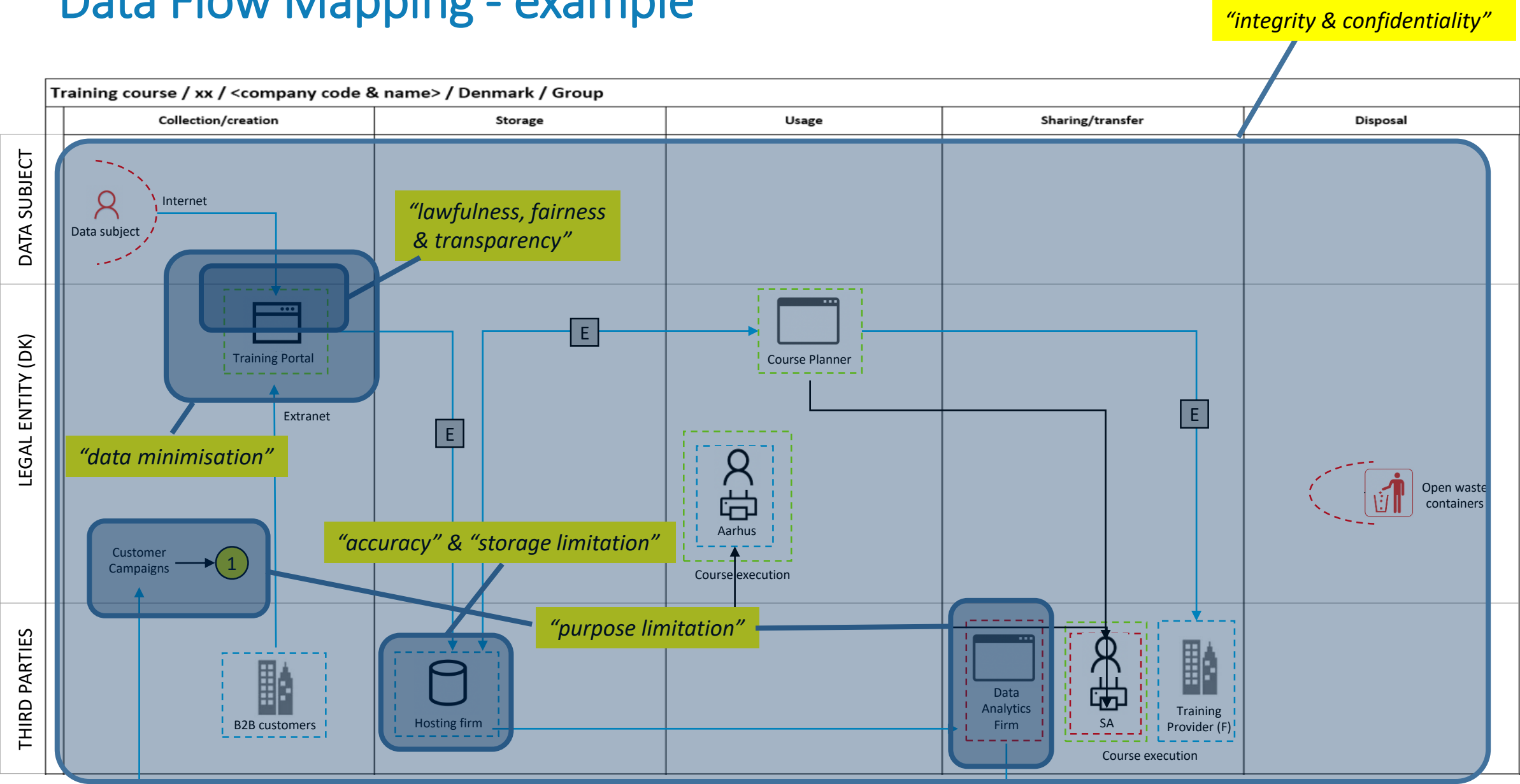
# Data flow mapping



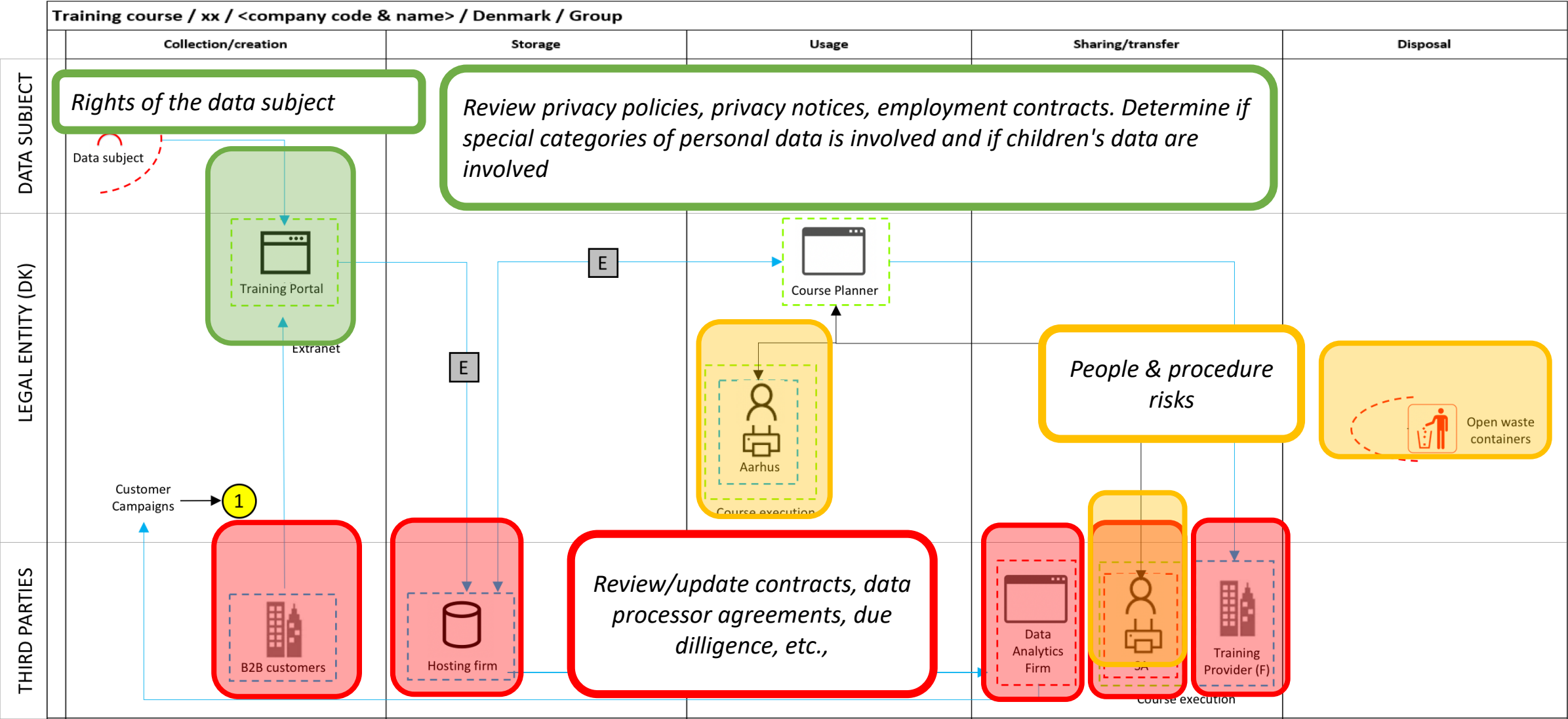
# Data Flow Diagram – key concepts



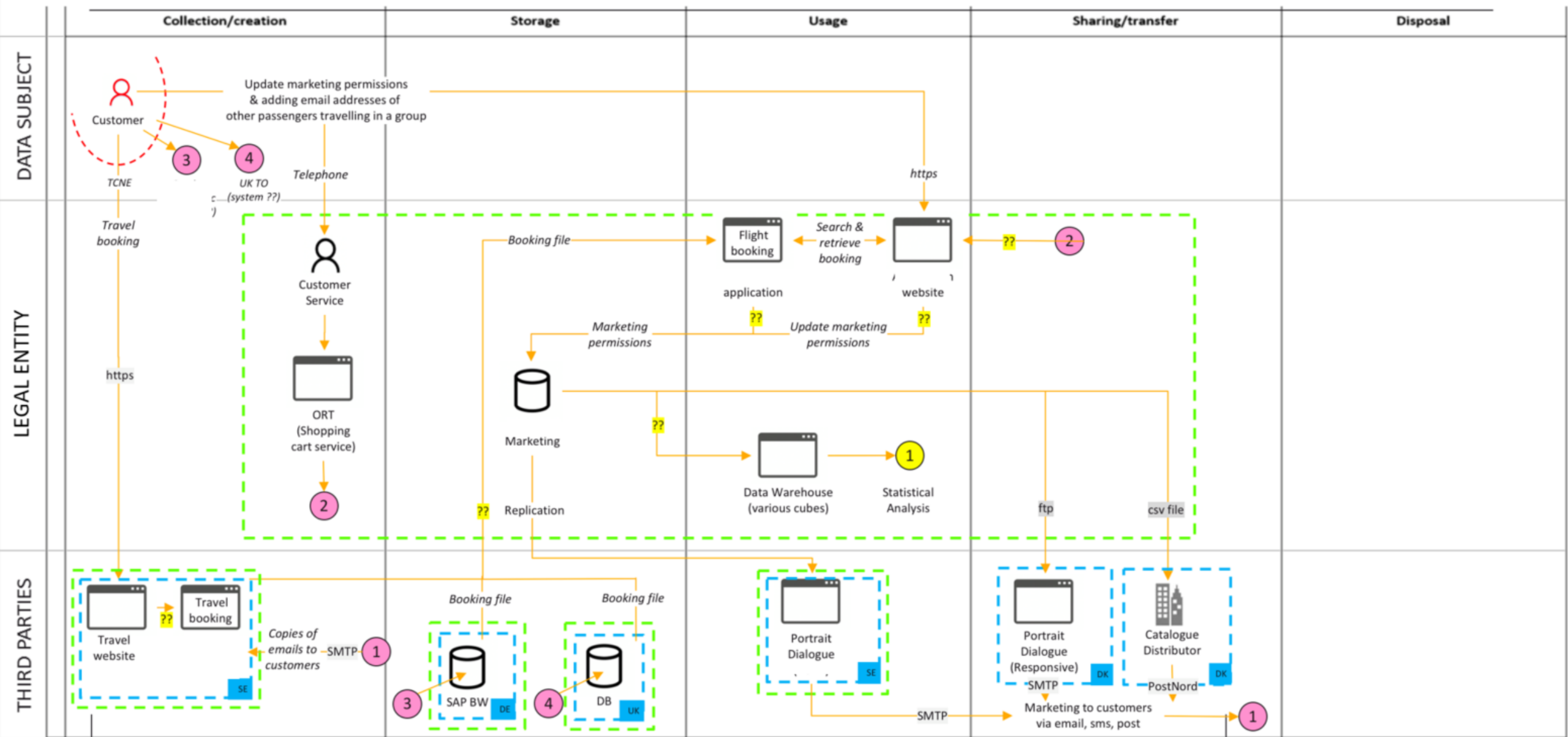
# Data Flow Mapping - example



# Data Flow Mapping - example



# EXAMPLE



# Data flow elicitation techniques

Information about as-is data flows can be elicited using various techniques and combinations of them.

Some people are more comfortable with one than another. Some like to share knowledge, others don't. Some prefer to be visual, liner, physical etc.



Inspect existing documentation



Facilitated workshops with SMEs



Interviews with key resources



Questionnaires



Observation



Physical data flow walk through

**Pros:**

- Avoid time/effort documenting
- Reduce disturbing busy colleagues
- Useful if key resources are missing

**Cons:**

- May not exist
- May be out-to-date
- May not reflect what's really happening

**Pros:**

- Consistent structure
- Can gather end-to-end input quickly if everyone's available
- Teamthink – also good to reach consensus
- Saves time for the team in gathering individuals

**Cons:**

- Sometimes perceived as resource intensive
- Knowledge gaps if everyone is not available
- Extra effort in capturing information

**Pros:**

- Formal or informal
- Focused dialogue
- Builds relationships

**Cons:**

- Skill needed to capturing information
- Time consuming for the team
- Not good at reaching consensus about a data flow

**Pros:**

- Elicit information from large groups of people
- Focused
- Easier analysis for closed questions

**Cons:**

- Analysis can be time consuming if questions are open-ended
- Not so good for building relationships

**Pros:**

- Ability to spot good/bad habits or behaviours
- Can get clarification by asking immediately
- Good to spot environmental and behaviour aspects

**Cons:**

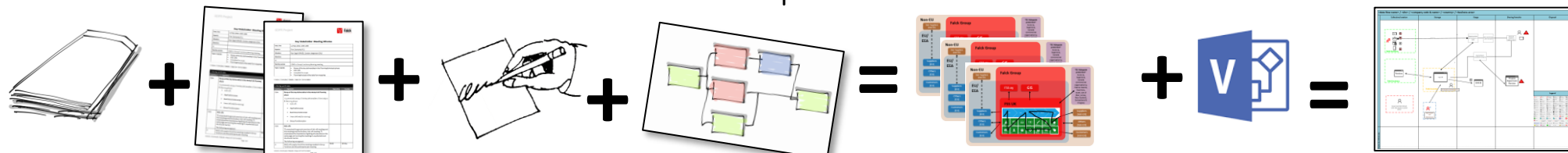
- Can be negatively disruptive
- Time consuming

**Pros:**

- Practical understanding and context
- Good to spot environmental aspects
- Builds relationships
- Sometimes easier to remember (physical experience)

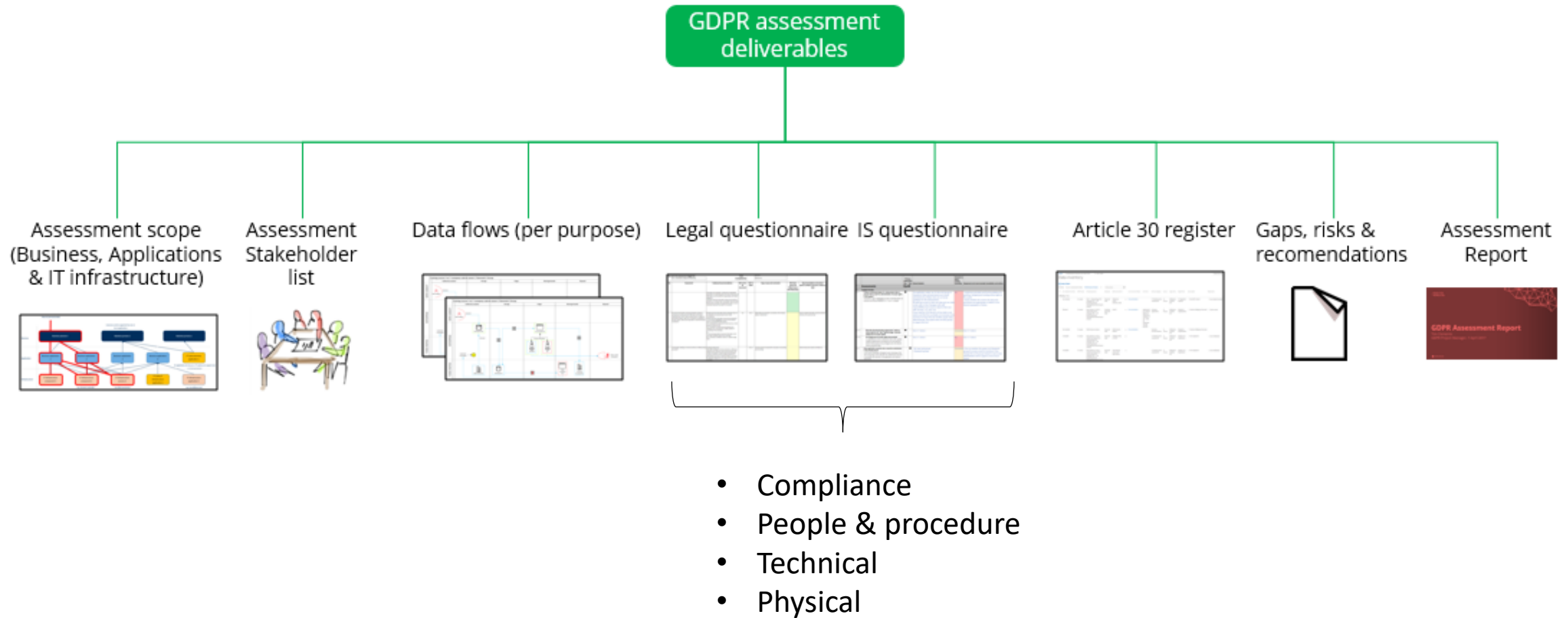
**Cons:**

- Time consuming
- Extra effort in capturing information

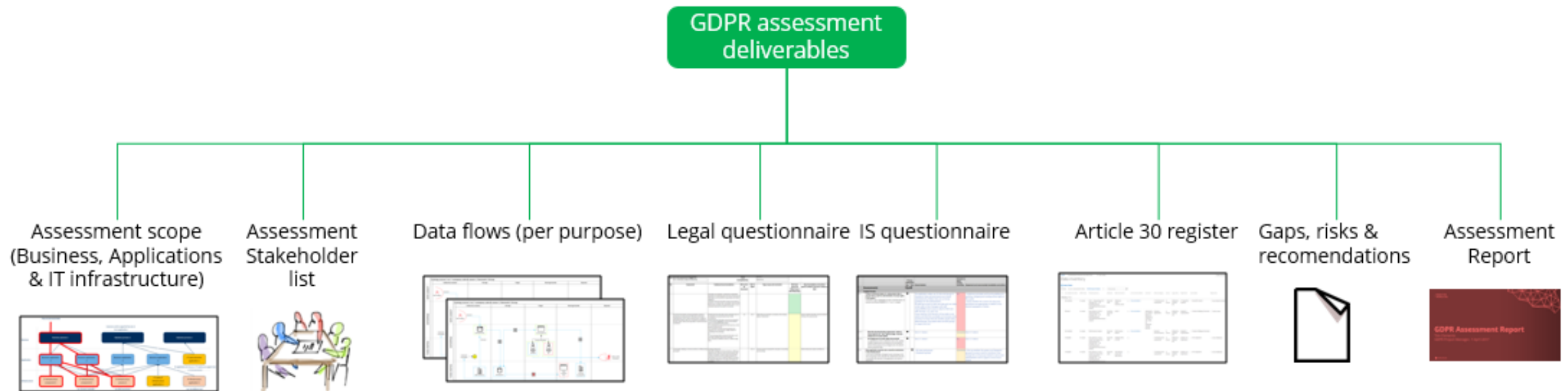




# As-is assessment – key deliverables



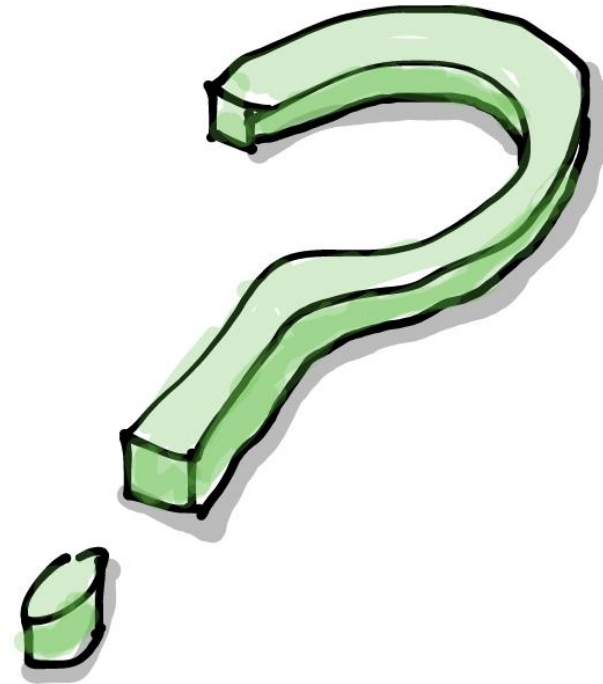
# Assessment – deliverables and competences



## Minimal assessment team:

- Workshop facilitator (Business Analyst/Process Consultant)
- Legal SME (Privacy Lawyer)
- Information Security SME

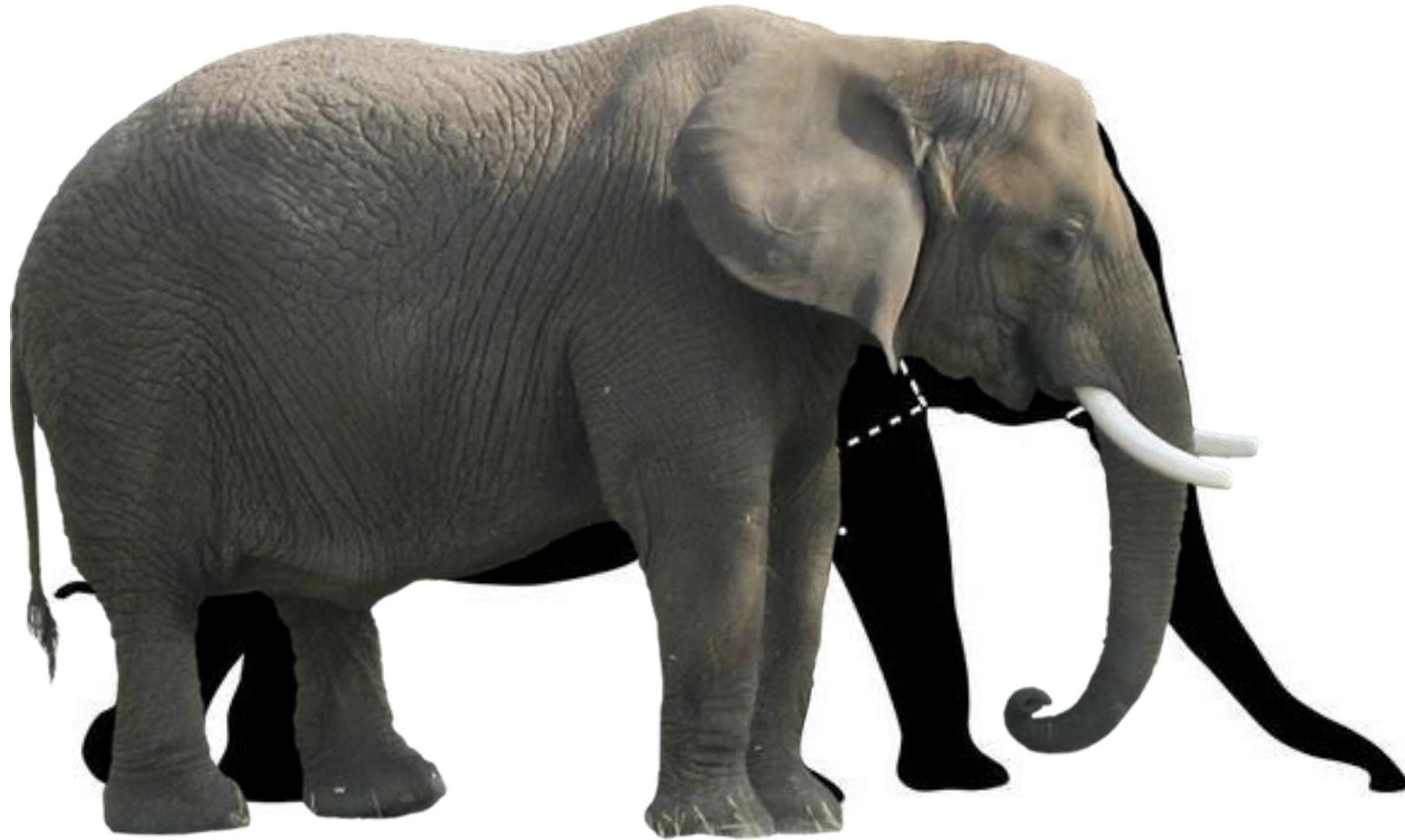
Remember to  
submit questions via  
the Q&A function



Identifying  
project scope



## Identifying project scope



# Identifying project scope – how to start



How does GDPR impact these perspectives in your organisation?



New or amended processes, procedures and functions



Changes to, or new organisational roles & responsibilities, staffing levels, skills and culture



Changes to, or new technologies, tools, IT applications, IT infrastructure

Contracts, Data Processor Agreements, Policies, Consent Records, Privacy Notices etc., etc.

New or changes to information, agreements, contracts, data, documents, reports, records, etc.

# Project scope – example

GDPR Articles 35, 36 and 83 and Recitals 84, 89-96

*(1) Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall prior to the processing, carry out or commission a Data Protection Impact Assessment (DPIA) to assess the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.*

## Data Protection Impact Assessment



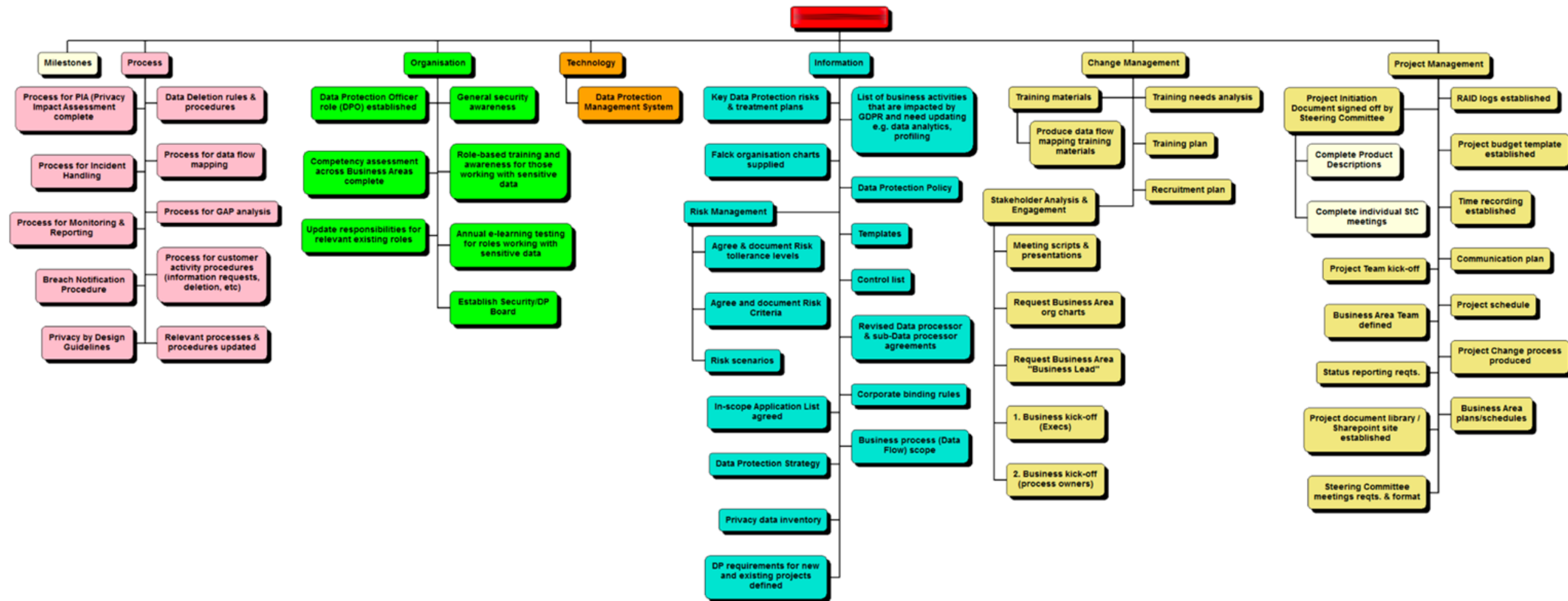
- Process for DPIA
- Embed in
  - Business case process
  - IT Change process
  - Project Management Method
- Etc

- Process owner
- Competences
  - Privacy risk
- Training
- Awareness
- Etc.

- DPIA repository
- Risk acceptance database
- Update CAB tools
- Etc

- Template
- Reporting
- Closure records
- Metrics
- Etc

# GDPR Project Deliverables Breakdown Structure



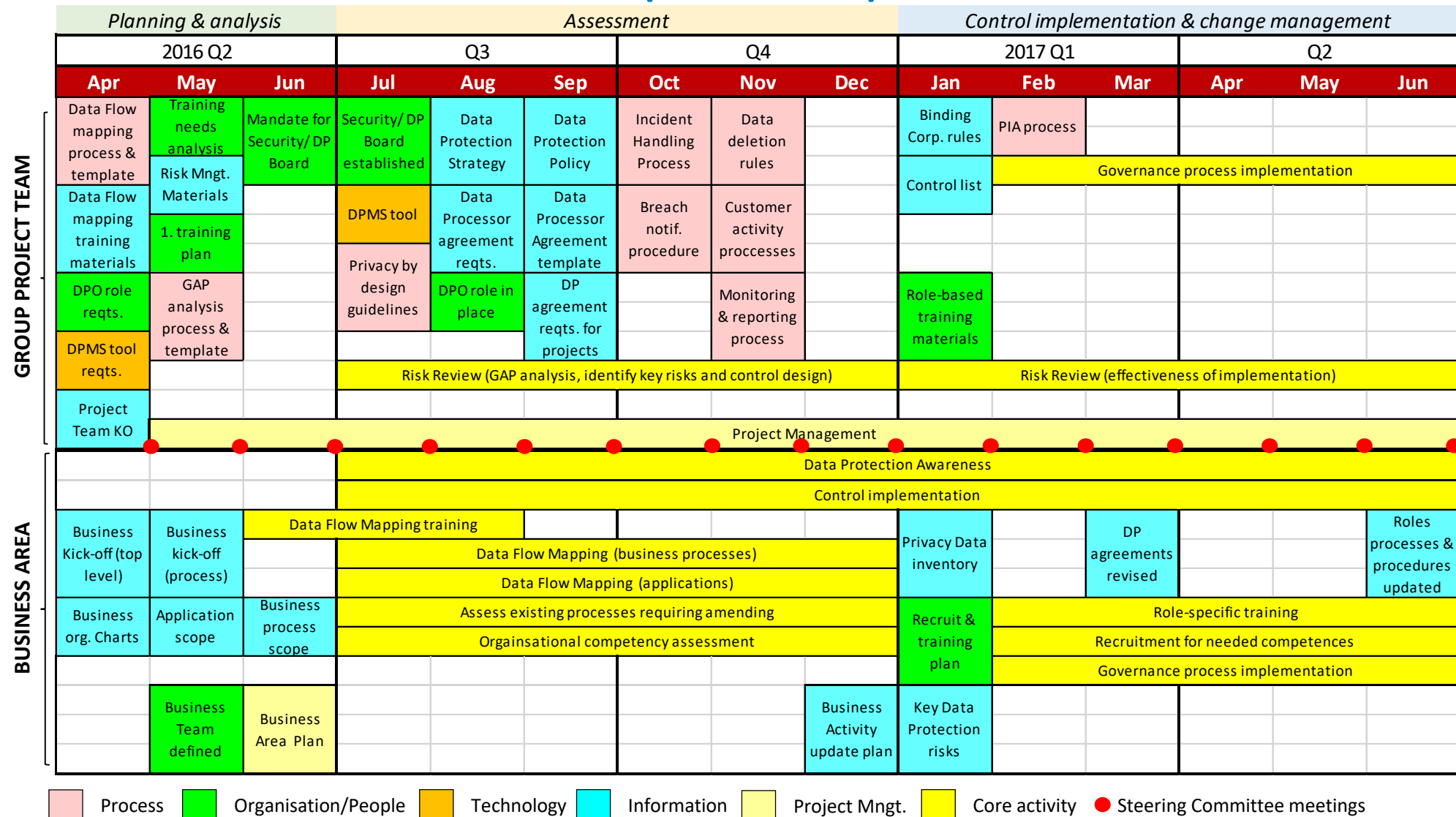


# GDPR Deliverables Roadmap – example 1

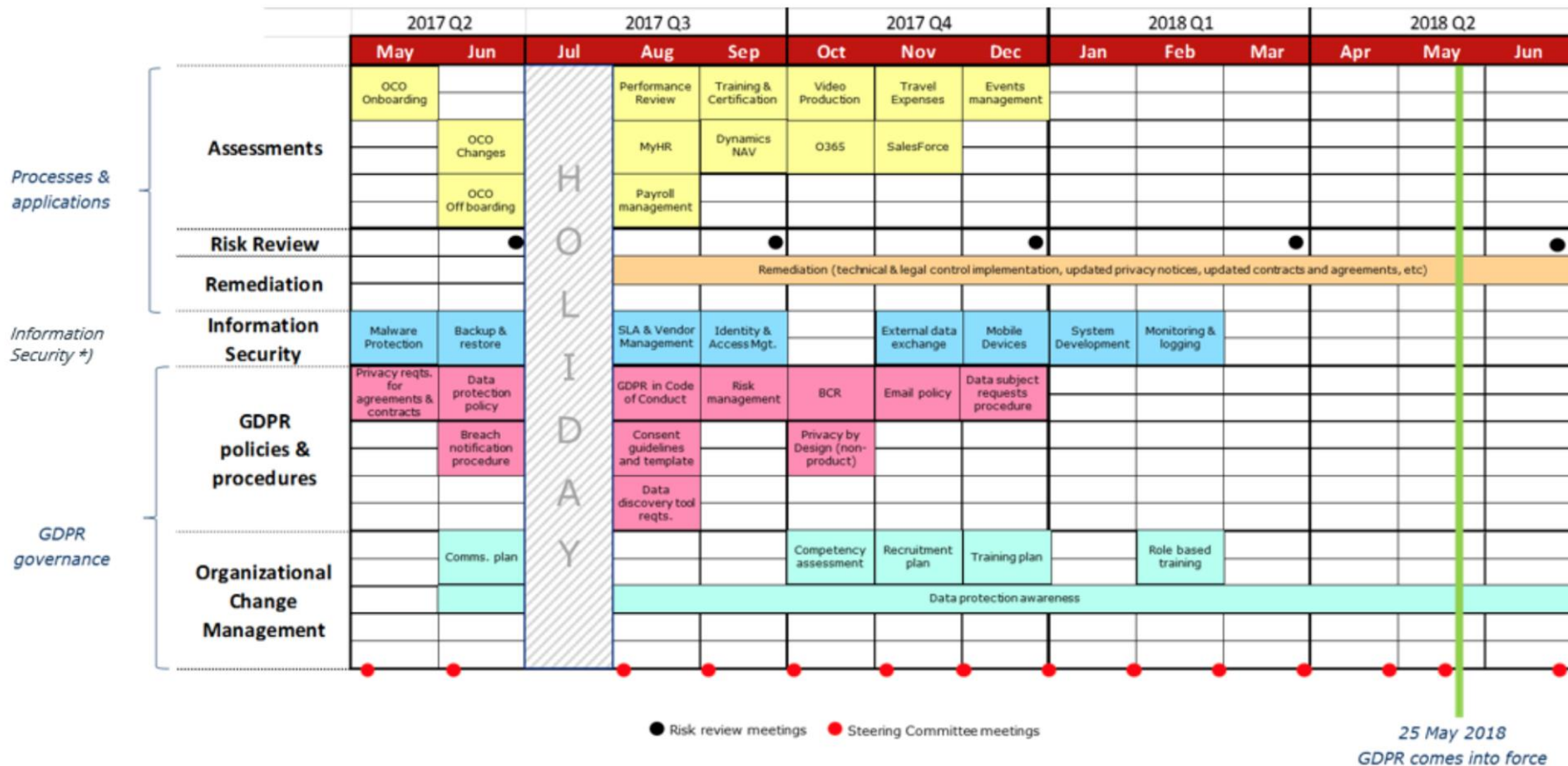
Prepare & plan			Pilot	Assessment						Control implementation & change management					
2017 Q1			2017 Q2			2017 Q3			2017 Q4			2018 Q1			
Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	
			Data protection awareness campaign												
Project team kick-off			Organizational competency assessment						Recruitment & training plan						
	Core team training														
Functional kick-offs									Role based training materials	Recruitment for needed competences					
Initial comms. & training materials										Role-specific training (sprints)					
					Assess inflight projects										
Data flow mapping procedure & template	Proof of concept	Pilot mapping & assessment		Revise data processor agreements & contracts (sprints)											
			Data flow mapping & Gap and Risk assessment (sprints)				Revise privacy notices & statements (sprints)				Readiness reviews & tests				
			Data protection policies, procedures & control implementation (sprints)												
	Legal & IS Assessment questionnaire		Audit & compliance policy	Compliance standards				Business process update plan	Update business processes (sprints)						
			Information management policy	Data processor standards & agreements	Data use procedures		3 <sup>rd</sup> party data exchange agreements	Privacy data inventory	Privacy notice inventory	DP agreement inventory					
	Data protection strategy	Data protection policy	Information classification procedure	Privacy by design procedures	Data collection procedures		Data portability procedures	Gap & risk list	Monitoring & reporting procedures	Internal audit procedures	Binding corporate rules				
Process & application scope	Risk Management materials		Document & record control policy	DP impact assessment procedures	Data quality procedures		Data disposal procedures	Information notices procedures		Due diligence & 3 <sup>rd</sup> parties audit procedures					
DP management system reqts.		DP management system implemented	Public trust charter		Subject access procedures		Breach notification procedure	Incident handling procedure		Complaints procedures	Enforcement notices procedures				
Project portal & project document standards		Map InfoSec controls to GDPR													
			Information security policies, procedures & control implementation (sprints)												

Process, procedure
  Organisation/People
  Tool
  Information, data, documents
  Core activity
  Steering Committee meetings

# GDPR Deliverables Roadmap – example 2



# GDPR Deliverables Roadmap – example 3



## Data flow mapping procedure & template

## – Purpose

- **GDPR reference**

- \*5: Principles relating to processing of personal data; 22: Automated individual decision making, including profiling; 24: Responsibility of the controller; 25: Data protection by design and by default; 30: Records of processing activities; 32: Security of processing

The procedure will describe how to map the flow of personal data using standard procedure templates. The procedure will describe various elicitation approaches as well as how to complete the mapping template

The format of the template will be in Visio using vertical swim lanes for each stage of the data cycle.

**Due**

- ## Key tasks

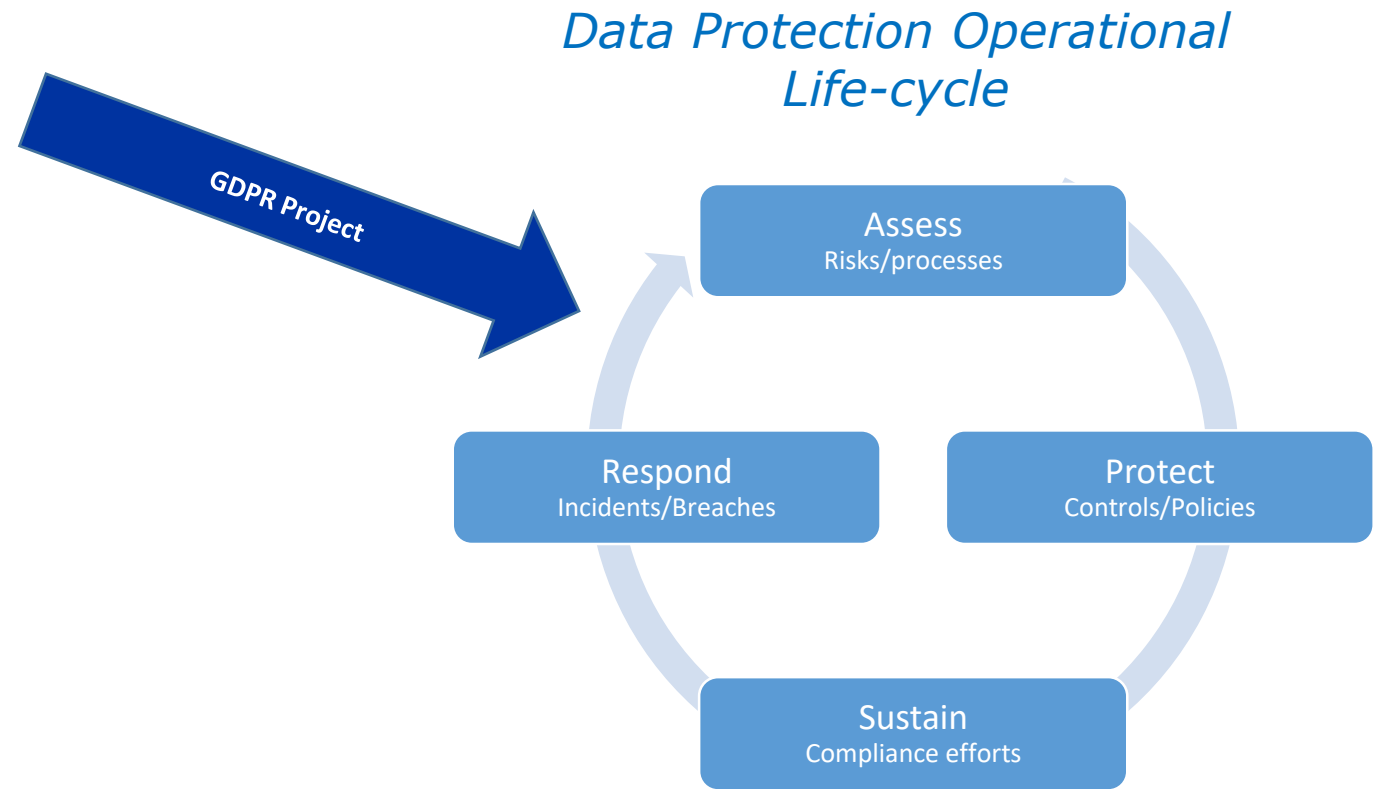
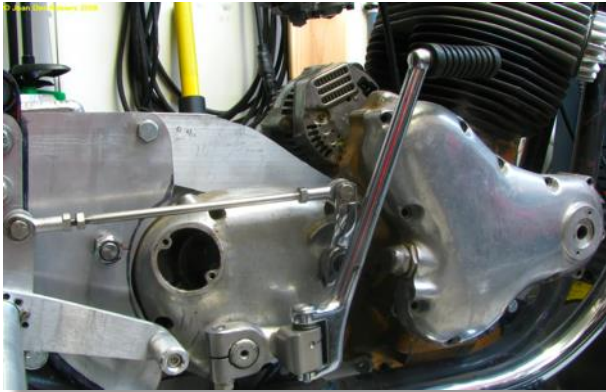
[illegible]

- None

**Sign-off responsible**

- \_\_\_\_\_

# Context of the GDPR Project



# Data protection operational lifecycle

Prepare & plan			Pilot	Assessment					Control implementation & change management						
2017 Q1				2017 Q2			2017 Q3		2017 Q4			2018 Q1			
Jan	Feb	Mar		Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar
				Data protection awareness campaign											
Project team kick-off	Core team training			Organizational competency assessment						Recruitment & training plan					
Functional kick-offs													Recruitment for needed competences		
Initial comms. & training materials													Role-specific training (sprints)		
				Assess in-flight projects											
Data flow mapping procedure & template	Proof of concept	Pilot mapping & assessment		Revise data processor agreements & contracts (sprints)											
				Data flow mapping & Gap and Risk assessment (sprints)					Revise privacy notices & statements (sprints)					Readiness reviews & tests	
				Data protection policies, procedures & control implementation (sprints)											
										Update business processes (sprints)					
	Legal & IS Assessment questionnaire			Audit & compliance policy	Compliance standards					Business process update plan					
				Information management policy	Data processor standards & agreements	Data use procedures				3 <sup>rd</sup> party data exchange agreements	Privacy data inventory	Privacy notice inventory	DP agreement inventory		
				Data protection strategy	Data protection policy	Information classification procedure	Privacy by design procedures	Data collection procedures		Data portability procedures	Gap & risk list	Monitoring & reporting procedures	Internal audit procedures	Binding corporate rules	
Process & application scope	Risk Management materials			Document & record control policy	DP impact assessment procedures	Data quality procedures				Data disposal procedures	Information notices procedures		Due diligence & 3 <sup>rd</sup> parties audit procedures		
DP management system reqs.		DP management system implemented		Public trust charter		Subject access procedures				Breach notification procedure	Incident handling procedure		Complaints procedures	Enforcement notices procedures	
Project portal & project document standards		Map InfoSec controls to GDPR													
Information security policies, procedures & control implementation (sprints)															

Process, procedure

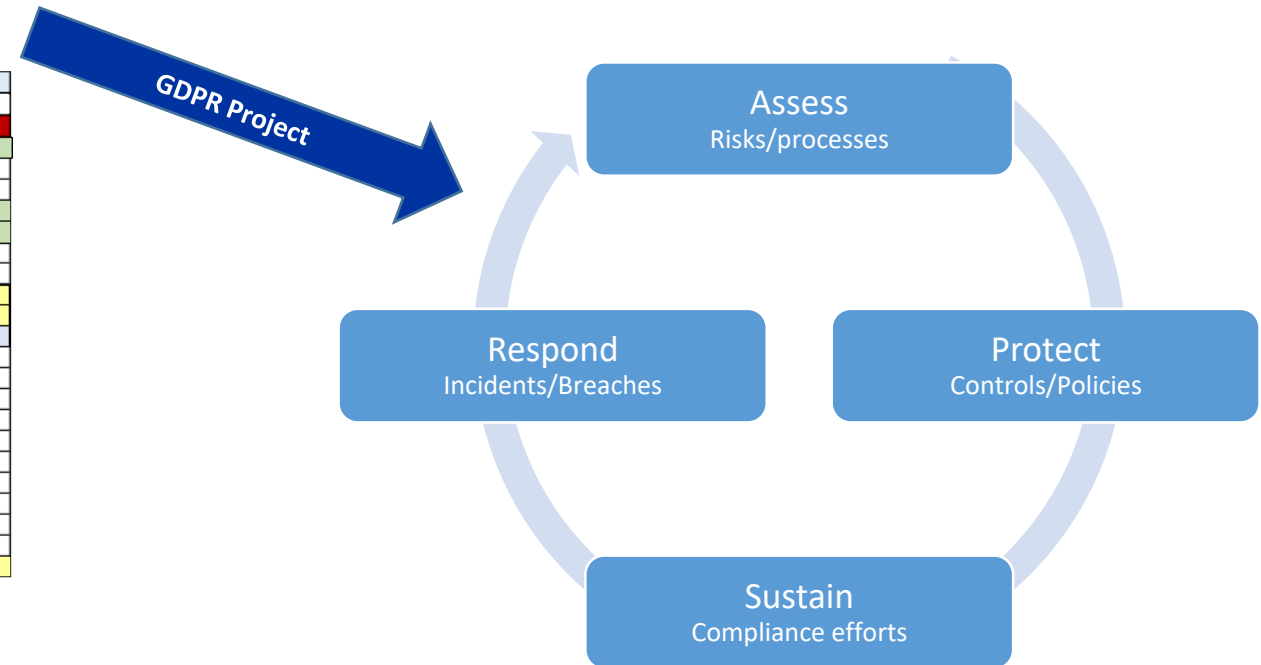
Organisation/People

Tool

Information, data, documents

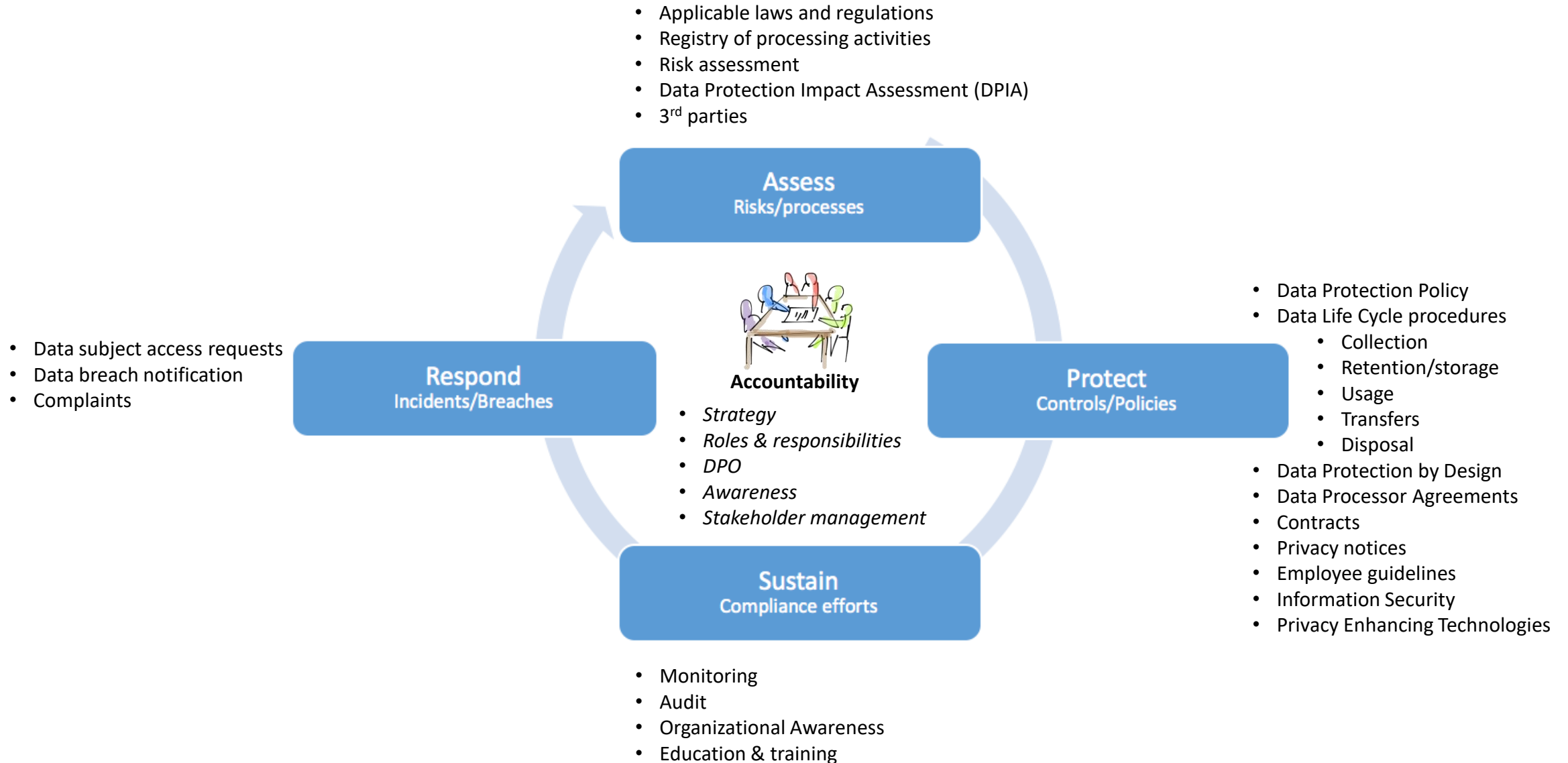
Core activity

Steering Committee meetings



*The project defines and implements a coherent set of policies, procedures, governance mechanisms and responsibilities to manage data protection and ensure ongoing compliance*

# Data Protection Operational Life Cycle





# Importance of ISO 27001

- Despite the few words in the GDPR, ISO 27001 (or other Information Security frameworks) is very important
- Mapping of 27001 Annex A controls to specific requirements has been performed
  - The Danish Confederation of Industries “Dansk Industri” (DI) offer a mapping in their GDPR Guideline document <sup>1</sup>
  - iso27001security.com have also performed a similar exercise <sup>2</sup>

<sup>1</sup> [http://digital.di.dk/SiteCollectionDocuments/Vejledninger/Persondataforordningen/Persondataforordningen\\_engelsk.pdf](http://digital.di.dk/SiteCollectionDocuments/Vejledninger/Persondataforordningen/Persondataforordningen_engelsk.pdf)

<sup>2</sup> <https://goo.gl/TpifBa>

# Other frameworks relevant to GDPR

ISO/IEC 27000 family -  
Information security  
management systems

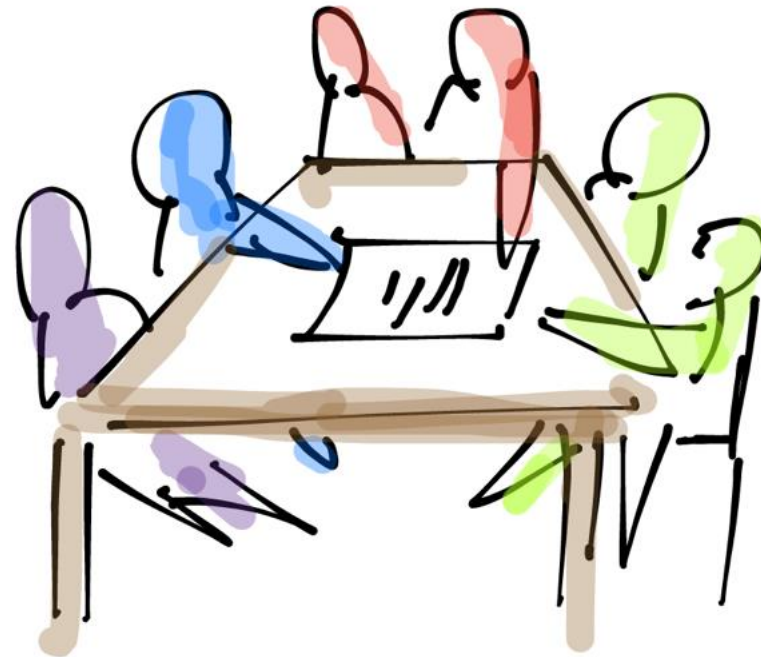
BS 10012:2017 – Personal  
Information Management  
System

NIST 800-53 Appendix J  
Privacy Controls

ISO 15489 – Information &  
documentation – records  
management



A slide for the  
busy executives



# Your Organisation's GDPR Project Game Plan

## Project scope

### Territorial scope

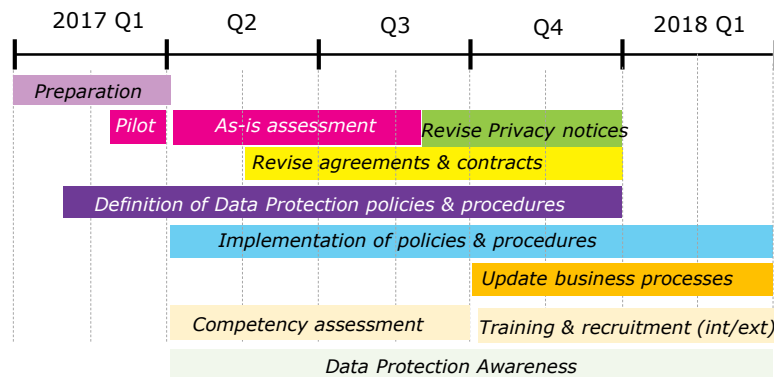
Global scope and includes processing activities by Your Organisation outside of the EU/EEA that target services to EU citizens, process EU citizen data (including employee data) or monitor data subjects' behaviour within the EU.

### Material scope

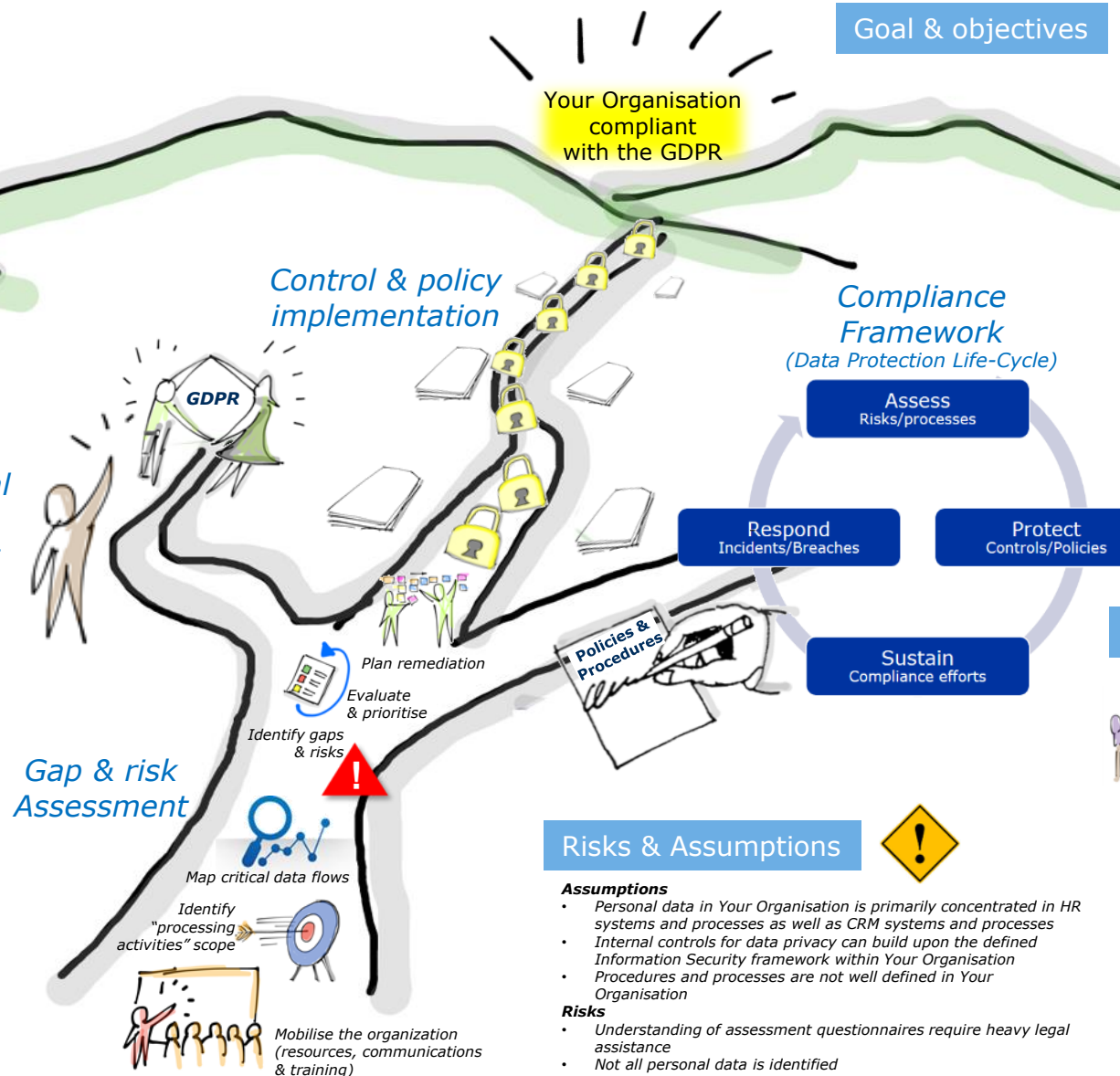
Personal data (any information relating to an identified or identifiable natural person) across the data life-cycle i.e. collected/created, stored, processed, shared and deleted.

## Organizational Change Management

## Timeline



## Gap & risk Assessment



## Goal & objectives

- Financial**
  - Reduce the risk of financial loss and reputational damage resulting from penalties & claims
- Customer**
  - Ability to demonstrate that Your Organisation's business is compliant with the GDPR
  - Ability to demonstrate Your Organisation is in control of personal data
  - Ability to act on the enhanced data subject rights
- Innovation**
  - Gain an overview of how and where personal data flows through Your Organisation's business system
  - Get an early view of data protection risks in new initiatives and projects

## Project organization

- Project Sponsor**
  - Sally Sixpack
- Steering Committee**
  - Joe Soap
  - Jens Hansen
  - Sven Svensson
  - Mario Rossi
  - Jane Doe
- Core project team**
  - Compliance
  - Legal
  - Procurement
  - HR
  - IT
  - Information Security
- External resources**
  - GDPR project support/advisor
  - Legal support
  - Information Security support

## Risks & Assumptions

### Assumptions

- Personal data in Your Organisation is primarily concentrated in HR systems and processes as well as CRM systems and processes
- Internal controls for data privacy can build upon the defined Information Security framework within Your Organisation
- Procedures and processes are not well defined in Your Organisation

### Risks

- Understanding of assessment questionnaires require heavy legal assistance
- Not all personal data is identified

Thank you  
for listening

Tim Clements

+45 6113 5106

[timclements@mac.com](mailto:timclements@mac.com)