CASTLEBRIDGE

Register of Processing Activities Masterclass

Practical Approaches to Developing, Maintaining, and Governance of a strategic resource

Course Outline

- 10 Modules
- Focus will be on ROPA as a *GOVERNANCE tool*
- Modules emphasise practical issues in data governance and change management relevant to the Article 30 question
- Modules will map the relationship of the ROPA to other elements of GDPR and other data-related regulatory functions.
- Breaks:
  - 11:00 (10 mins)
  - 12:40 (45 mins)
  - 14:40 (10 mins)

About Daragh O Brien BBLS, FICS, FIP, CDMP

- **Company**
  - Founder & CEO, Castlebridge (https://castlebridge.ie)
  - Working on business & people side of data since **1998**
  - Work with clients in public and private sector on data & information strategy, data governance, data protection compliance, AI strategy, data quality, data acumen/nous development
  - Also work with International Bodies such as the UN and EU Commission on regulatory and policy projects such as an AI Governance framework for a developing nation.
- **Industry**
  - Fellow of Irish Computer Society
  - Fellow of International Association of Privacy Professionals
  - Former board member/advisor to various professional bodies nationally/regionally/internationally (DAMA, IQ International)
  - Currently a contributing member to Leaders' Data Organisation (https://dataleaders.org)
  - Awarded Industry Recognition Award by IVI / Maynooth University in 2022 for over 20 years of contributions to Data Governance
  - Lifetime achievement award 2026 – Information & Records Management Society
  - Contributor to development of National Data Governance Roadmap for Ireland

About Daragh O Brien BBLS, FICS, FIP, CDMP

- **Education/Academia**
  - Degree in Business and Law, CDMP and various other certifications
  - Syllabus Consultant and Lecturer, Law Society of Ireland
  - Lecturer in Data Governance, Sutherland School of Law, University College Dublin
  - Guest Lecturer, School of Computing, Dublin City University
  - Lecturer with Public Affairs Ireland and the Institute of Public Administration
  - Advisory Member, Innovation Value Institute, Maynooth University
  - Member of Strategic Advisory Board, Maynooth University Business School
  - Doctoral Researcher, School of Engineering/LERO, University of Limerick

- **Books & Publications**
  - Author of several books / contributor to others on various data management topics
  - Co-author of *Ethical Data & Info Management* (2018) and *Data Ethics 2nd Edition* (2023)
  - Published several academic papers on topics such as data governance of drone-mounted sensor data
  - Contributing Author to DMBOK2.0
  - Featured columnist on TDAN.com since 2015.
  - My ORCID profile https://orcid.org/0009-0006-4864-5803

CASTLEBRIDGE

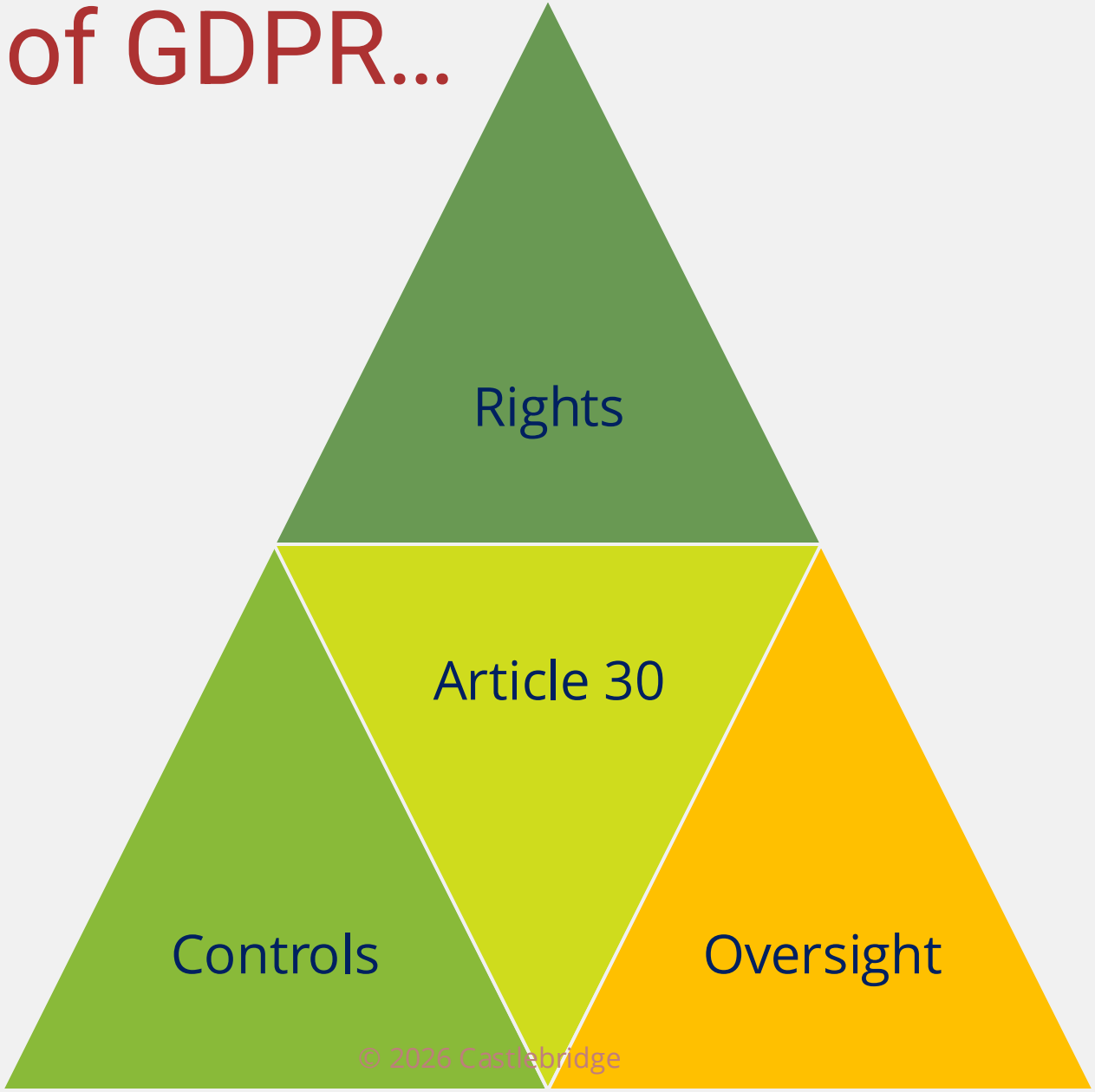
Module 1

Article 30 GDPR: Essential Overview

On completion of Module 1

Understand	Understand what the Article 30 ROPA is
Explain	Be able to identify • the minimum required information that must be included • the optional information that could be included
Understand	Be able to understand the ‘mandatory but not compulsory’ nature of ROPAs under GDPR
Recognise	Be able to recognise what is “good to see” in a ROPA
Identify	Identify common misconceptions and pain points experienced when developing and maintaining ROPAs

Article 30 of GDPR…



CASTLEBRIDGE

What does the legislation say?

- Obligations on both Controllers and Processors
- Important to know what role you are playing

Article 30

Records of processing activities

1. Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:

(a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;

(b) the purposes of the processing;

(c) a description of the categories of data subjects and of the categories of personal data;

(d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;

(e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;

(f) where possible, the envisaged time limits for erasure of the different categories of data;

(g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

2. Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing:

(a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;

(b) the categories of processing carried out on behalf of each controller;

(c) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;

(d) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

Controllers and Joint Controllers need to maintain a ROPA for the activities

Article 30 supports Article 26
(remember joint / severable liability of JCs)

Note:

- Different content requirements for ROPA for Controllers and Processors
- Not a generic template

Who needs to do a ROPA?

- Recital 13 and Article 30(5)
  - Rec. 13:
    - *"To take account of the specific situation of micro, small and medium-sized enterprises, this Regulation includes a derogation for organisations with fewer than 250 employees with regard to record-keeping"*
  - Art 30(5):
    - *"The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10"*

Myth: Small organisations don't need to do a ROPA

- Under 250 staff you are exempt from doing a ROPA unless…

1. The processing activity is not "occasional", or
2. The processing is likely to result in a **risk** to the rights and freedoms of Data Subjects, or
3. The processing relates to Special Category data or data relating to criminal convictions/offences

For any of these, you MUST maintain a ROPA for the processing activities that fall within these parameters

REGARDLESS OF HOW MANY STAFF YOU HAVE

EDPB Guidance on Article 30 Registers is explicit…

Therefore, although endowed with less than 250 employees, data controllers or processors who find themselves in the position of either carrying out processing likely to result in a risk (not just a high risk) to the rights of the data subjects, or processing personal data on a non-occasional basis, or processing special categories of data under Article 9(1) or data relating to criminal convictions under Article 10 **are obliged to maintain the record of processing activities.**

WORKING PARTY 29 POSITION PAPER on the derogations from the obligation to maintain records of processing activities pursuant to Article 30(5) GDPR

Things Data Controllers MUST record

MUST Element	Legal Basis and Commentary
Name and contact details of controller	Art. 30(1)(a). Also include joint controller, representative, and DPO where applicable.
Purposes of processing	Art. 30(1)(b). Must be specific and meaningful, not generic statements.
Categories of data subjects	Art. 30(1)(c). Types of individuals (employees, customers, patients, etc.).
Categories of personal data	Art. 30(1)(c). DPC emphasises "granular and meaningful" detail required.
Categories of recipients	Art. 30(1)(d). Including recipients in third countries or international organisations.
International transfers	Art. 30(1)(e). Third country identification and documentation of safeguards.
Time limits for erasure	Art. 30(1)(f). "Where possible" qualifier applies. Different retention periods for different data categories.
Security measures description	Art. 30(1)(g). "Where possible" and "general description" qualifiers apply.
Written form	Art. 30(3). Must be in writing, including electronic form.
Availability to supervisory authority	Art. 30(4). Must be made available on request. DPC expects availability within 10 days.

Things Data Controllers SHOULD record

SHOULD Element	Source/Rationale	GDPR Connection
Lawful basis for processing	ICO Accountability Framework; DPC lists as "helpful extra" information	Art. 6 (and Art. 9 for special categories). Enables Art. 13/14 transparency.
Art. 9 condition (special category data)	DPC guidance; ICO Accountability Framework	Art. 9. Where special category data processed, condition must be documented.
Source of personal data	Required for Art. 14 compliance where data not obtained from data subject	Art. 14(2)(f). Transparency requirement where indirect collection.
Transfer mechanism	ICO guidance; enables demonstration of lawful transfer basis	Art. 46/49. SCCs, adequacy, BCRs, or derogation must be identifiable.
Organisational structure (by function)	DPC guidance: "break down the RoPA with reference to different functions"	Supports accountability demonstration under Art. 5(2).
Link to data protection notice	ICO recommendation; enables consistency verification At a minimum you need to be able to demonstrate that there is a relationship between what's in the ROPA and what's in your Data Protection Notice	Art. 13/14. ROPA content should align with transparency disclosures.
Regular review/update process	DPC: "regular reviews... should be carried out"; ICO: "living document"	Art. 5(2). Accountability requires current, accurate records.
Standalone document	DPC: "The RoPA is a standalone record... not [a DPIA]"	Art. 31. Must be accessible to supervisory authority without interpretation.

Things you COULD (might) record

COULD Element	Governance Value
Risk ratings per processing activity	DPC lists risk ratings as "helpful extra information." Enables prioritisation of governance effort and supports risk-based approach.
Data breach history	DPC lists "whether a breach has occurred" as helpful extra information. Links processing activities to incident history.
System/application inventory	Links processing activities to specific systems where data is held. Supports subject access request fulfilment and incident response.
Data steward/owner identification	Assigns accountability for each processing activity. Supports broader data governance and accountability requirement
Data quality indicators	Documents known quality issues or dependencies. Connects data protection to broader data governance.
Change history/audit trail	Records when and why ROPA entries were modified. Demonstrates ongoing governance attention.
Cross-references to related processing	Links related processing activities (e.g., marketing and customer service). Supports holistic understanding of data flows.
Automation/profiling indicators	Flags processing involving automated decision-making. Supports Art. 22 compliance assessment.

Doesn’t have to be in the ROPA itself – but worth considering as part of BROADER governance!

Processors?

- Similar considerations for the “Should” and “Could”
- Must:
  - Who do you process data for
  - What do you process it for?
  - What type of processing activity do you do?
  - How do you secure it
  - Does it travel outside EEA?

Why doesn’t a processor have to define a period for retention of the personal data in their ROPA?

The Key Questions for Both

What DPC considers “good”

Guidance: Records of Processing Activities (RoPA) under Article 30 GDPR
An Coimisiún um Chosaint Sonraí Data Protection Commission

Requirement	Requirement Type	Example A	Example B	Insufficient Example	Recommendation
Name and contact details of the controller	Required	Example company Building, Road, Town, County, Eircode 045 XXX XXX info@examplecompany.ie	Example company Town, County, Eircode 045 XXX XXX info@examplecompany.ie	John.doe@examplecompany.ie	Full contact details of the controller to be supplied. Personal emails are not recommended due to personnel changes.
Name and contact details of the joint controllers	If relevant		NA		
Name and contact details of the controller's representative	If relevant		NA		
Name and contact details of the Data Protection Officer	Required	John Doe dpo@examplecompany.ie 045 XXX XXX	External DPO company dpo@examplecompany.ie ExampleCompanyDPO@externalcompany.ie	John.doe@externalcompany.ie	Full contact details of the DPO to be supplied. If an external DPO is used, clarity to be provided and full details supplied
Purposes of processing	Required	HR—Payroll	Protected Disclosures Receipt and Investigation	HR	Purpose of processing should be granular enough so that only the personal data required are processed
Description of the categories of data subjects	Required	Temporary staff Permanent staff	Discloser of information Any persons named in disclosure Witnesses Any other person identified during investigation	All	Separation of different categories of staff, or different types of service user, customers, potential customers etc. is recommended where relevant to different processing activity types. Categories of data subject may include identifying where the processing of vulnerable person's data is to take place
Description of categories of personal data	Required	Name, employee number, PPSN, location, hours worked, remuneration, employee bank details, leave information, deductions	Name, employee ID, personal contact details, work contact details Additional categories of personal data may be required dependent on the nature of the disclosure. These will be recorded in the disclosure record.	Personal data	The actual data processed should be recorded
Categories of recipients to whom the personal data have been or will be disclosed	Required	Revenue, employee bank, Dept. of Social Protection (as required)	On a case-by-case basis: The Protected Disclosures Commissioner An Garda Síochána or other relevant law enforcement authorities if offences are discovered Legal advisors Anonymised report required to be published annually	Internal	The data controller should be in a position to know and to demonstrate to whom personal data will be shared
Time limits for erasure of the different categories of data	If possible		7 years post completion, archived securely after 1 year	As per retention policy	Where available, specifics should be included
General description of the technical and organisational measures referred to in Article 32(1)	If possible		Secure reporting system pursuant to the Protected Disclosures (Amendment) Amendment Act 2022 Systems uses 2 factor authorisation Only trained and designated personnel have access to the PD system	GDPR compliant	This is an opportunity to demonstrate the measures taken to ensure the security of personal data processing carried out
Where personal data may be disclosed or otherwise transferred to a third country or an international organisation			NA		
Categories of recipients to whom the personal data have been or will be disclosed in other country/organisation	Required	NA	NA		
The name of the country or international organisation	Required	NA	NA		
The documentation of suitable safeguards in the case of Article 49(1) transfers	If relevant	NA	NA		
Lawful basis	Recommended	Article 6(1)(b) and (c) Article 9(2)(b)	Article 6(1)(c) Protected Disclosures Act 2014 Protected Disclosures (Amendment) Act 2022	Article 6	
For all entries on the RoPA, should the data controller wish to link to other governance documents in order to better demonstrate compliance, or to provide clarity, the links should work outside the data controllers IT environment or the additional documentation must be supplied to the DPC at the same time as the RoPA, if requested.					

CASTLEBRIDGE

The Slane Decision (DPC)

- Due to technical error, documentation held in the “Director’s Area” on the Slane CU website was exposed and indexed by search engines over approx. a 1 week period in November 2018
- This included “Member Enquiry Reports” containing personal data of 76 people including 34 children.
- DPC commenced an investigation in 2019, among the issues for investigation was whether Article 30 had been breached.

A key summation of what's required…

7.3. Thus, Articles 24 and 30(1) both envisage the implementation by controllers of certain policies and records. It is clear from the listed criteria set out in Article 30(1) for inclusion in a record of processing, and from the specific factors to which a controller must have regard under Article 24(1) that those provisions envisage the accurate identification by the controller of the nature of personal data processed by them, in addition to the purposes for which they are processed. Consequently, in order to meet the requirements of those provisions, and to effectively demonstrate compliance with the GDPR, a controller's data protection records and policies must accurately reflect the processing of personal data by that controller. In that vein, they must be maintained as living documents that are updated to take account of any developments to the processing operations of the controller.

Data Inventory vs Register of Processing

- Record of Processing Activity needs to capture context.
- Processing activities can happen on paper
- Processing activities can happen outside the “core” IT systems
- Need to answer some core interrogatives
  - What?
  - Why?
  - Where?
  - Who?
  - When?
  - How?

Unclear what level of “data inventory” Slane CU had done and if it actually included all the things needed for a robust ROPA

CASTLEBRIDGE

ROPA as a “Data Flow Map” or “Data Map”

- ROPA does not record data flows
- ROPA is not a mapping of where data is.
- ROPA records what things are done with data
- It can…
  - Record *where* that processing happens and where data is held
  - Record *how* data moves between functions
- This is a *BYPRODUCT of the metadata recorded in a ROPA process*

CASTLEBRIDGE

Module 2

The Register of Processing Activities as a Data Governance Artefact

On completion of this module

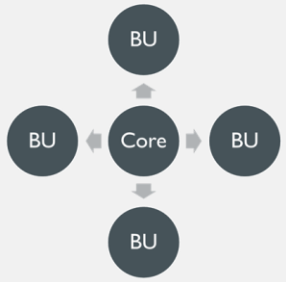
Explain	Be able to explain what data governance is and how it relates to data protection
Understand	Understand how Data Governance supports ROPA
Understand	Understand how ROPA enables Data Governance
Explain	How Article 30 ROPA links to Article 24, Article 25, Article 32, Article 33, and other obligations under GDPR
Identify	Identify how Data Governance model affects design choices for delegation of ROPA granularity, responsibility and accountability

Defining Data Governance

"The focus of Data Governance is on how decisions are made about data, and how people and processes are expected to behave in relation to data"

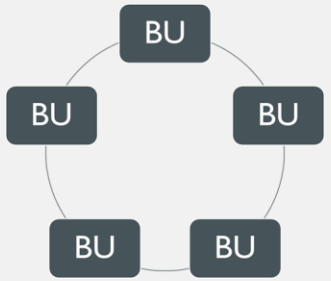
- DAMA DMBOK, Chapter 3

Models for Data Governance



Centralised

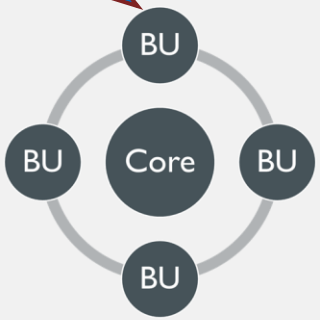
- Consistent approach
- Can take time to recognise issues/errors
- One size may not fit all scenarios
- Difficult to change
- Less responsive
- “Work arounds” are inevitable



Decentralised

- Highly localised approach
- No central view of all activities
- Impossible to standardise work practices
- Coordination is ad hoc at best
- Inconsistent responses to data subjects
- Depends on local team knowledge and skills

Useful for large organisations or orgs with semi-independent business units



Hybrid

- Balanced approach
- Central view with local concerns addressed
- Variations are identified and documented
- Formal and informal co-ordination methods
- Consistent and timely responses to Data Subjects
- Depends on local team knowledge and skills

Data Governance and Data Protection

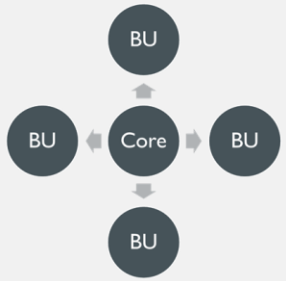
Data Protection Concept	Description	Role in Governance
Data Protection Officer	A defined senior management role responsible for oversight of Data Protection Compliance and independent voice in issue management.	Point of escalation for issues, co-ordinates with Regulator, "Conscience of the organisation"
Data Processor (Contracts with)	Data Controllers are required to have formal agreements in writing with 3rd parties processing data on their behalf; Processors acting outside bounds of contract can be prosecuted as Controllers	Define scope of what is to be done by Processor; Requires formal Change Control on how 3rd Parties handle personal data.
Joint Controllers (Documentation of Joint Controller Relationship)	Two or more Data Controllers jointly defining the purpose and means for processing personal data; Requires formal documentation of roles and responsibilities; Determines where penalties fall in event of a breach of the legislation; "Essence" of agreement must be published	A RACI document that outlines who is doing what (and, ultimately, who pays for what to be done). Essential part of managing day to day operational issues and avoiding conflict
Categories of personal data	Three categories exist in GDPR: Personal, Special Categories, and Data relating to Criminal offences or prosecution. Important to know what kind of data you are dealing with.	General Data Classification is a good practice for Information governance; Extends beyond personal data to include commercially sensitive information as well.
Documentation of Processing Activities	Formal requirement to document processing activities involving personal data; Article 30 spells out specific information that must be recorded, including data classifications, data sources, 3rd party processors, lawful basis for processing etc	Good Process Governance requires documentation of critical activities to ensure they are executed consistently in the organisation; Can reduce training time/costs if processes are documented properly.
Requirement for defined Procedures for Data Subject Rights	Formal requirement to define standardised processes for the handling of requests from Data Subjects for the exercise of their rights. Processes must be documented, and it is a breach not to do so.	As above: to ensure appropriate and consistent responses when timeframes for response are tight and control required over process, standardisation is Essential
Accountability Principle	The principle that Data Controllers (and Processors) will be process data in compliance with the Regulation and will be able to demonstrate that compliance	Good governance is evidenced based with preventative, detective, and remedial controls. Development of KPIs for Data Protection is a recommended practice.

How ROPA supports Data Governance

How Data Governance Supports ROPA

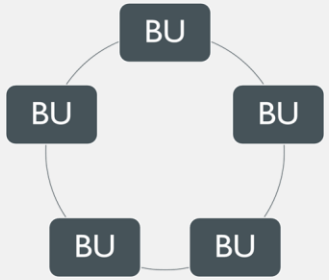
- **Responsibility** for creation
- **Accountability** for maintenance and updating
- **Delegation** of functions
- **Standardisation** of approaches
  - Terminology
  - Processes
  - Categories of data / data subject / purpose
- **Remediation** of differences

Models for Governance of ROPA



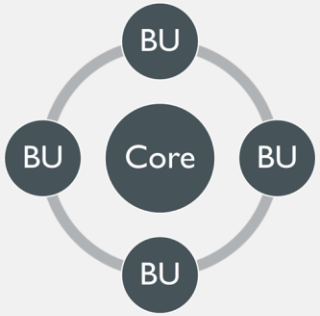
Centralised

- Consistent approach
- Can take time to recognise issues/errors
- One size may not fit all scenarios
- Difficult to change
- Less responsive
- “Work arounds” are inevitable



Decentralised

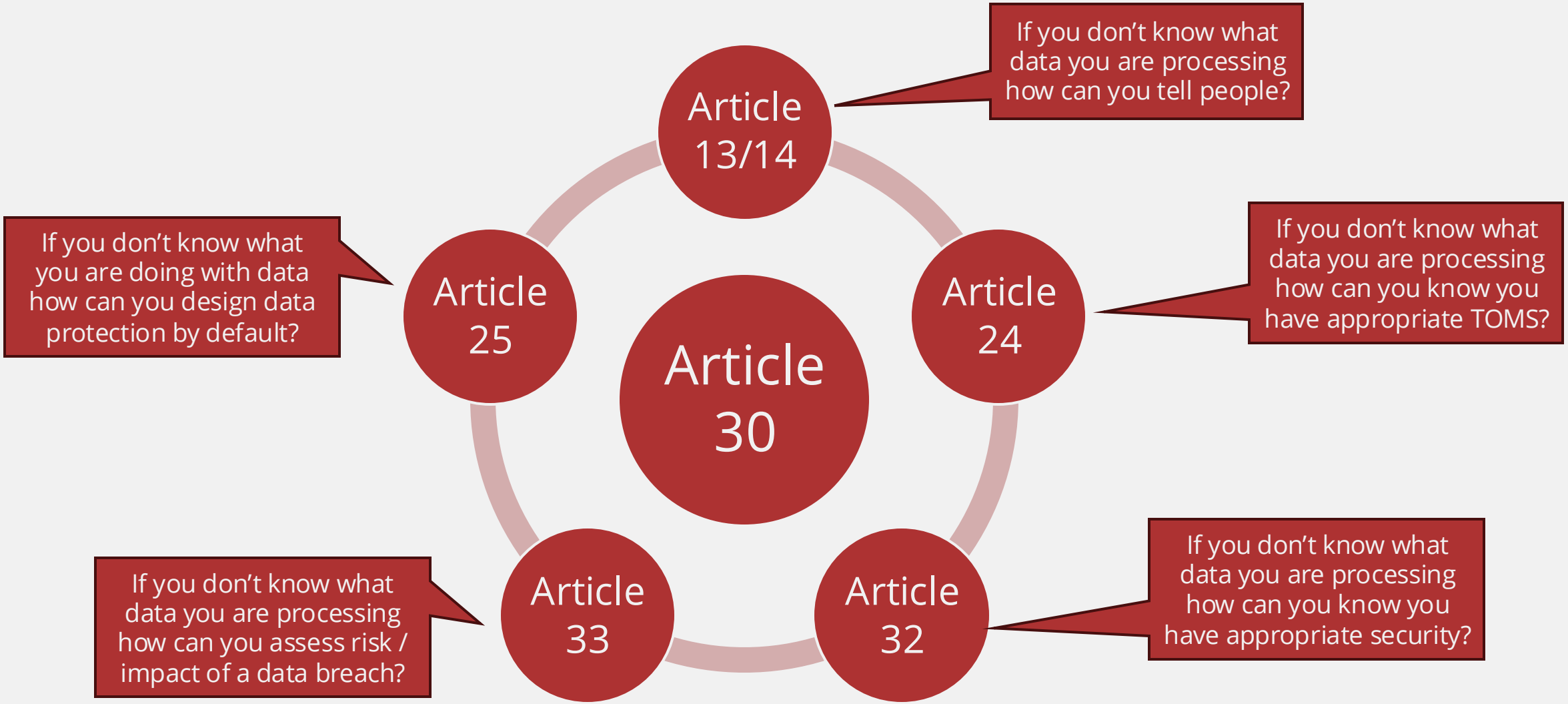
- Highly localised approach
- No central view of all activities
- Impossible to standardise work practices
- Coordination is ad hoc at best
- Inconsistent responses to data subjects
- Depends on local team knowledge and skills



Hybrid

- Balanced approach
- Central view with local concerns addressed
- Variations are identified and documented
- Formal and informal co-ordination methods
- Consistent and timely responses to Data Subjects
- Depends on local team knowledge and skills

Relating ROPA to other obligations



A Quality Systems View

If you cannot describe what you are doing as a process then you don't know what you are doing.
(W. Edwards Deming)

CASTLEBRIDGE

Module 3

The Article 30 Register of Processing Activities as a Metadata Hub

On completion of Module 3

Understand	Understand the concept of metadata and how the ROPA functions as a structured repository of metadata
Identify	Identify the categories of metadata captured in a ROPA and map to broader GDPR governance obligations
Explain	Explain relationship between other metadata registers and governance artefacts and how the ROPA acts as a “hub”
Understand	How metadata helps enable and support accountability
Explain	Explain how ROPA should be a “living document” as a metadata hub

What is Metadata?

- The DAMA Data Management Body of Knowledge (DMBOK) defines metadata simply as **"data that provides information about other data."** It is the descriptive layer that gives data its meaning, context, and governance structure.
- Three categories of metadata:
  - **Business metadata** describes the meaning and use of data from an organisational perspective. It includes definitions, business rules, data ownership, applicable policies, and regulatory context. In a GDPR context, the legal basis for processing, the purpose of a processing activity, and the categories of data subjects are all business metadata.
  - **Technical metadata** describes the structural and system-level properties of data — schemas, data types, field lengths, system of record, data models, and lineage. In a GDPR context, this encompasses the IT systems in which personal data is held, how data flows between systems, and the technical security measures applied.
  - **Operational metadata** describes how data is used in practice over time — job execution logs, record volumes, access histories, data quality metrics, and retention lifecycle events. In a GDPR context, operational metadata includes retention periods, deletion logs, transfer records, and breach notifications.

ROPA as Metadata Repository / Hub

Article 30 Element	Metadata Category
Name of Controller	Business Metadata
Contact Details of Controller	Business Metadata
Joint Controller Name	Business Metadata
Contact Details of Joint Controller	Business Metadata
Controller's Nominated Representative	Business Metadata
Contact Details for Nominated Representative	Business Metadata
Data Protection Officer	Business Metadata
Contact Details for DPO	Business Metadata
Purposes for Processing	Business Metadata
Categories of Data Subject	Business Metadata
Categories of Personal Data	Business Metadata
Categories of Recipients	Business Metadata
Third Country Transfers	Operational Metadata
Time Limits for Categories of Data	Operational Metadata
Technical Security Controls Description	Operational Metadata
Organisational Security Controls Description	Operational Metadata

The Key Questions

Metadata = Categories

Article 30

Records of processing activities

1. Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:

(a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;

(b) the purposes of the processing;

(c) a description of the categories of data subjects and of the categories of personal data;

(d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;

(e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;

(f) where possible, the envisaged time limits for erasure of the different categories of data;

(g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

2. Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing:

(a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;

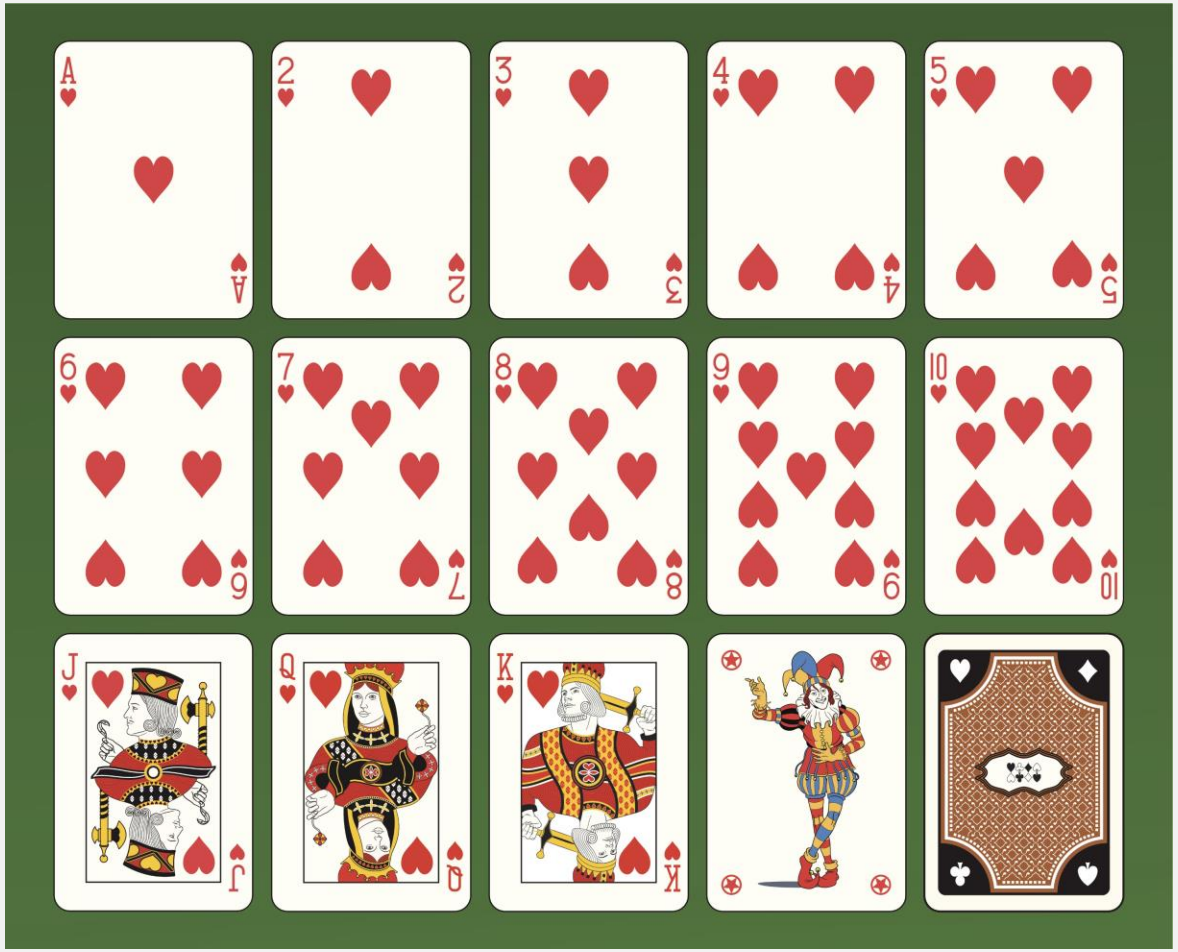
(b) the categories of processing carried out on behalf of each controller;

(c) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;

(d) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

Benefits of Thinking in terms of categories

Categories And Classifications of data in GDPR

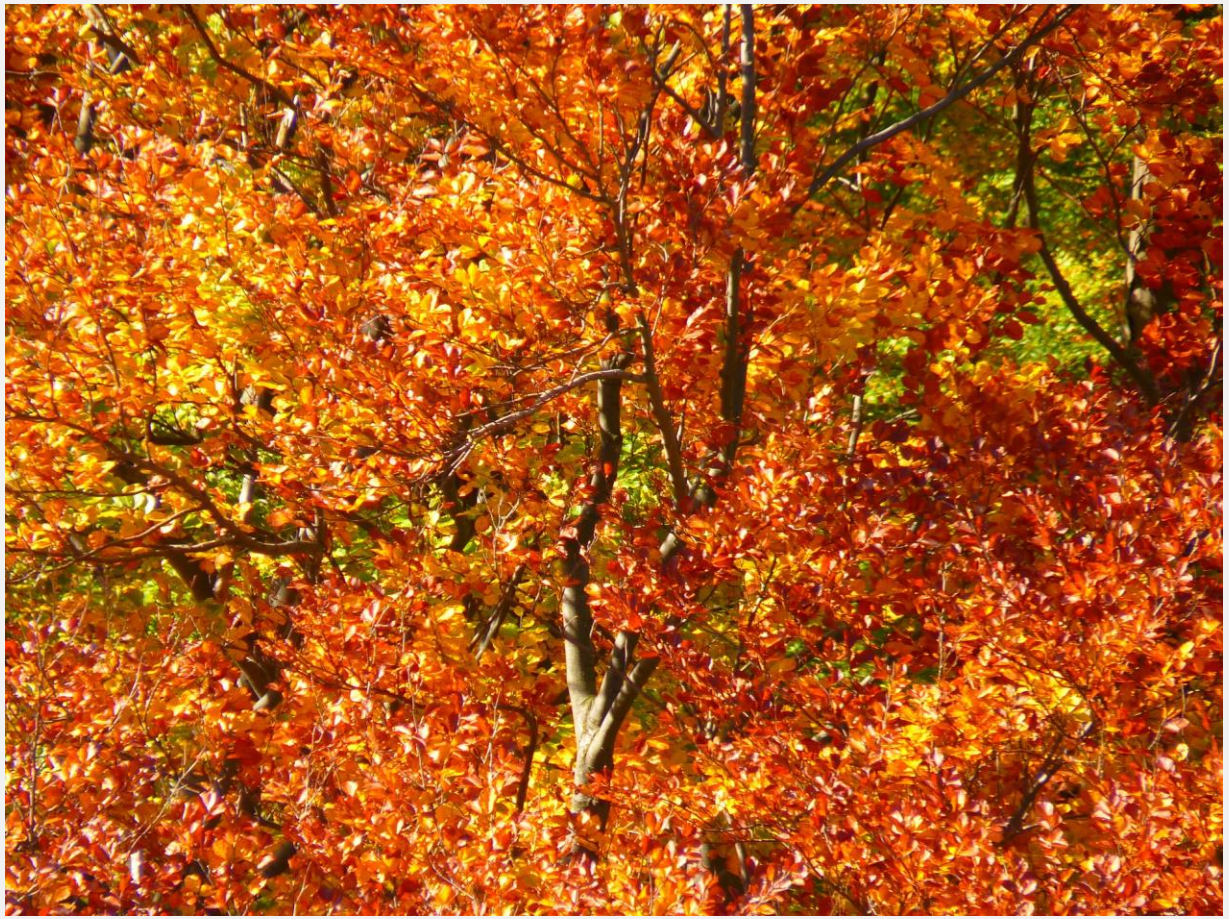


Categories of Data Subject

- Important for risk classification
- Who do you process data about?
- What labels do you put on them?
- What do those labels mean?
- Does the label change at the end of a process?

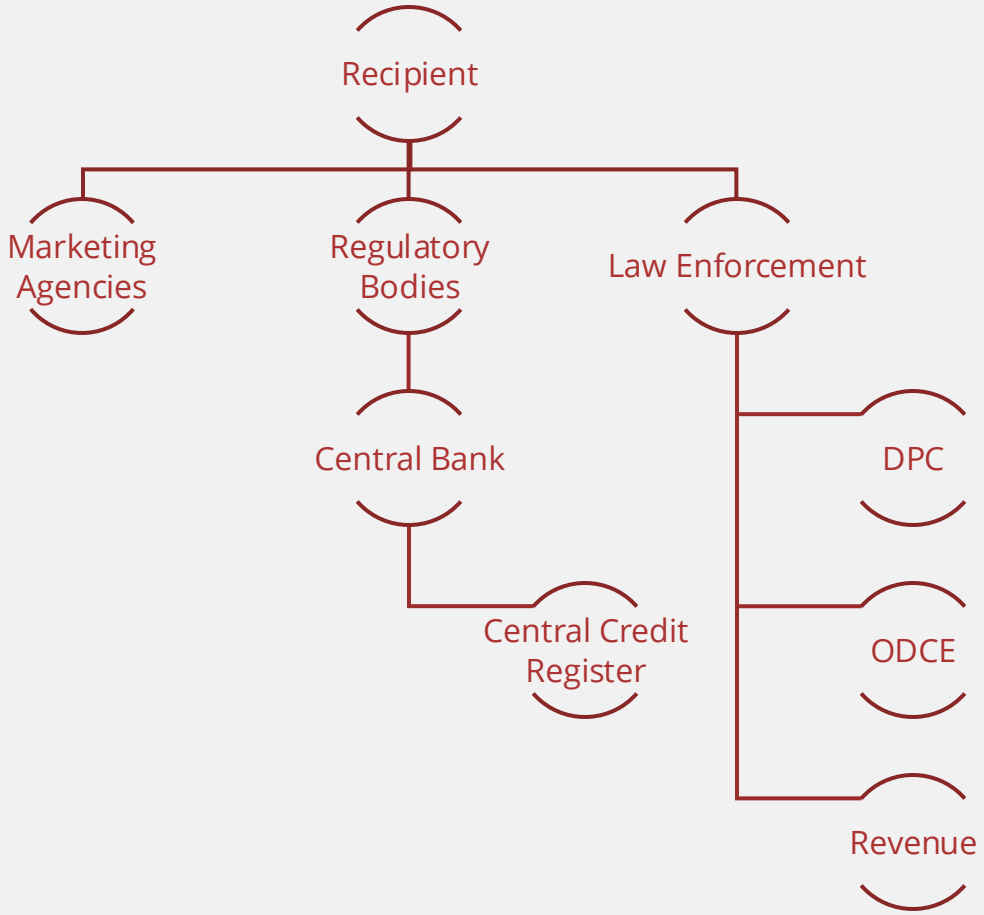
CASTLEBRIDGE

The Important Thing…
Get out of the DETAIL!!



- See the wood for the trees
- Bring documentation up to a useable level of detail
- Support *consistency* in drill down to lower levels of detail

Categories of Recipient



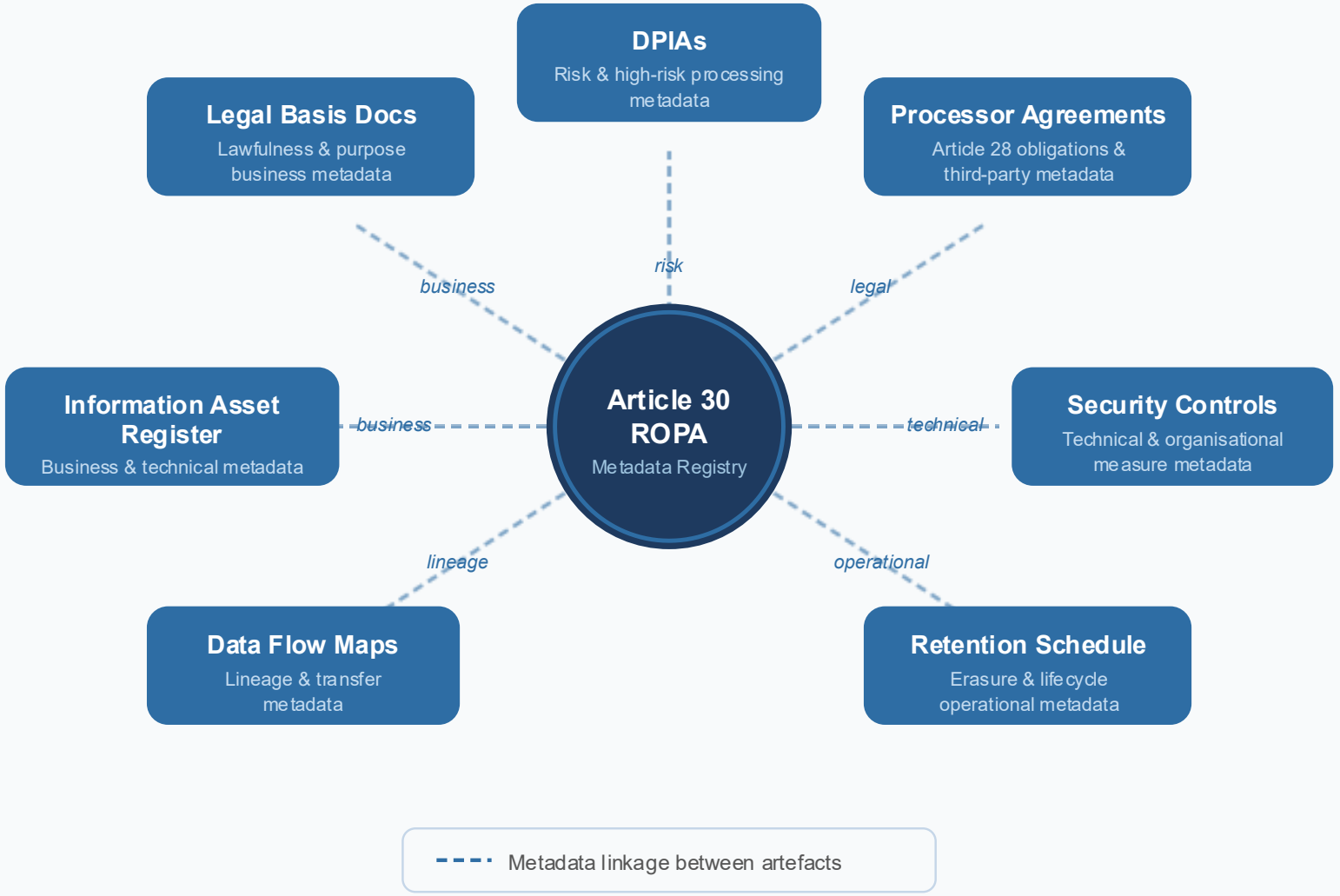
Recipient:
A Natural or Legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not… (Article 4 GPDR)

- Who do you share data with?
- What categories and classifications of bodies are they?
- Are any of them conducting inquiries under EU or Member State law?
- What other categories of Recipient might your organisation have to deal with?

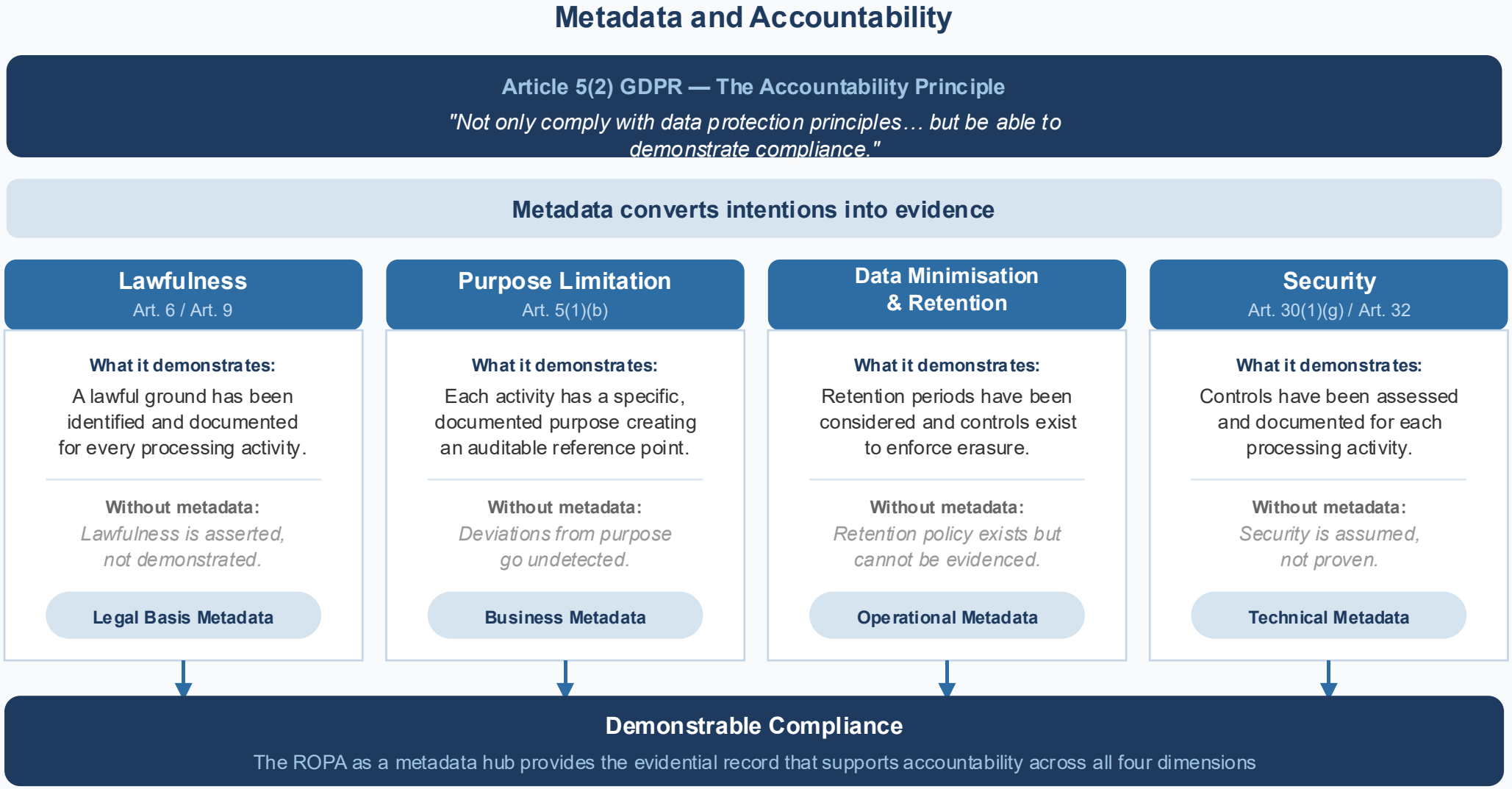
Exercise

- You are developing a ROPA for a high street retailer
- Identify the categories of data subject about whom the retailer might process personal data across their functions
  - Retail stores
  - Online stores
  - Loyalty card scheme

ROPA as a Metadata Hub



Metadata and Accountability



CASTLEBRIDGE

Module 4

What is a “Processing Activity” anyway?

On completion of Module 4

Understand	Understand what a “processing activity” actually is
Identify	Identify the characteristics of a processing activity as opposed to a function of the organisation
Explain	Explain how to identify processes in the organisation
Understand	Understand the importance of Verb-Noun language when discussing processing activities
Explain	Explain how identifying processing activities can help map flows of data across organisation

Why Process Modelling is Essential

- W. Edwards Deming: “If you can’t describe what you’re doing as a process, you don’t know what you’re doing”. *Out of the Crisis*, 1986
- Alec Sharp: “A process that is not defined is nothing more than a vicious rumour that somewhere someone is supposed to be doing something” (on a conference panel at IRMUK EDBIA conference, 2010).

Article 30 requires documentation of "processing activities," yet many organisations struggle to define what constitutes a processing activity and how to identify them comprehensively.

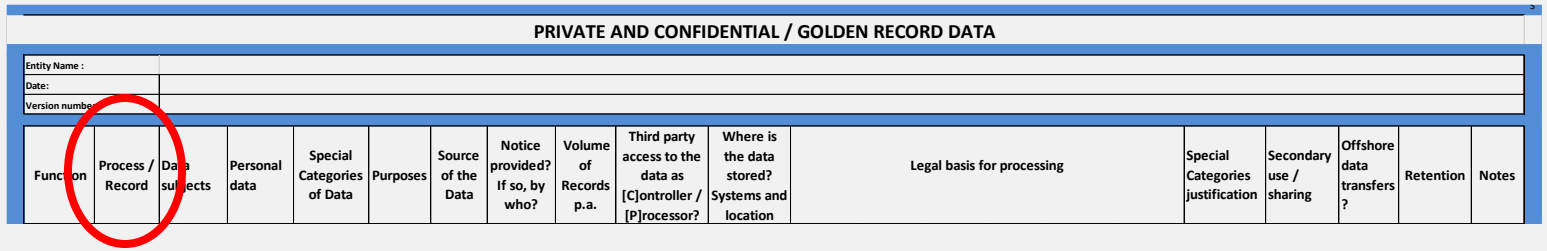
CASTLEBRIDGE

TRAC Methodology (Alec Sharp)

- Trigger:
  - What starts the process off? What are the actions / temporal triggers, or other conditions that start (or stop) the processing?
- Results:
  - What are the outcomes to be delivered by the process? When is it “done”? These should be discrete and countable things.
- Activities:
  - What is done? What are the major **activities** (5-7 major things) that need to be done to achieve the result?
- Cases:
  - Are there variations to the process or scenarios that must be handled? For example CCTV footage in a retailer may capture images of customers, visitors, and “suspects”. Identification of cases can help refine ROPA documentation so it captures full scope of processing.

What is a process?

A defined sequence of steps and decisions, to achieve a particular result
Alec Sharp



PRIVATE AND CONFIDENTIAL / GOLDEN RECORD DATA

Entity Name :	
Date:	
Version number:	

Function	Process / Record	Data subjects	Personal data	Special Categories of Data	Purposes	Source of the Data	Notice provided? If so, by who?	Volume of Records p.a.	Third party access to the data as [C]ontroller / [P]rocessor?	Where is the data stored? Systems and location	Legal basis for processing	Special Categories justification	Secondary use / sharing	Offshore data transfers ?	Retention	Notes

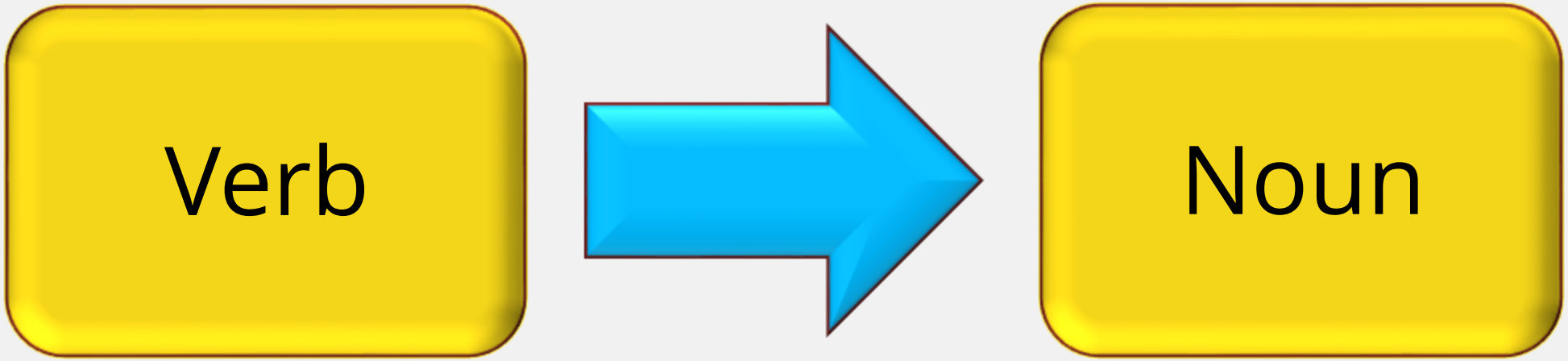
Trigger Event → Workflow [Steps and Decisions] → Outcome / Result

Verb-Noun naming
“Acquire Customer”

Noun-Verb naming
“Customer Acquired”

CASTLEBRIDGE

The Importance of Grammar…



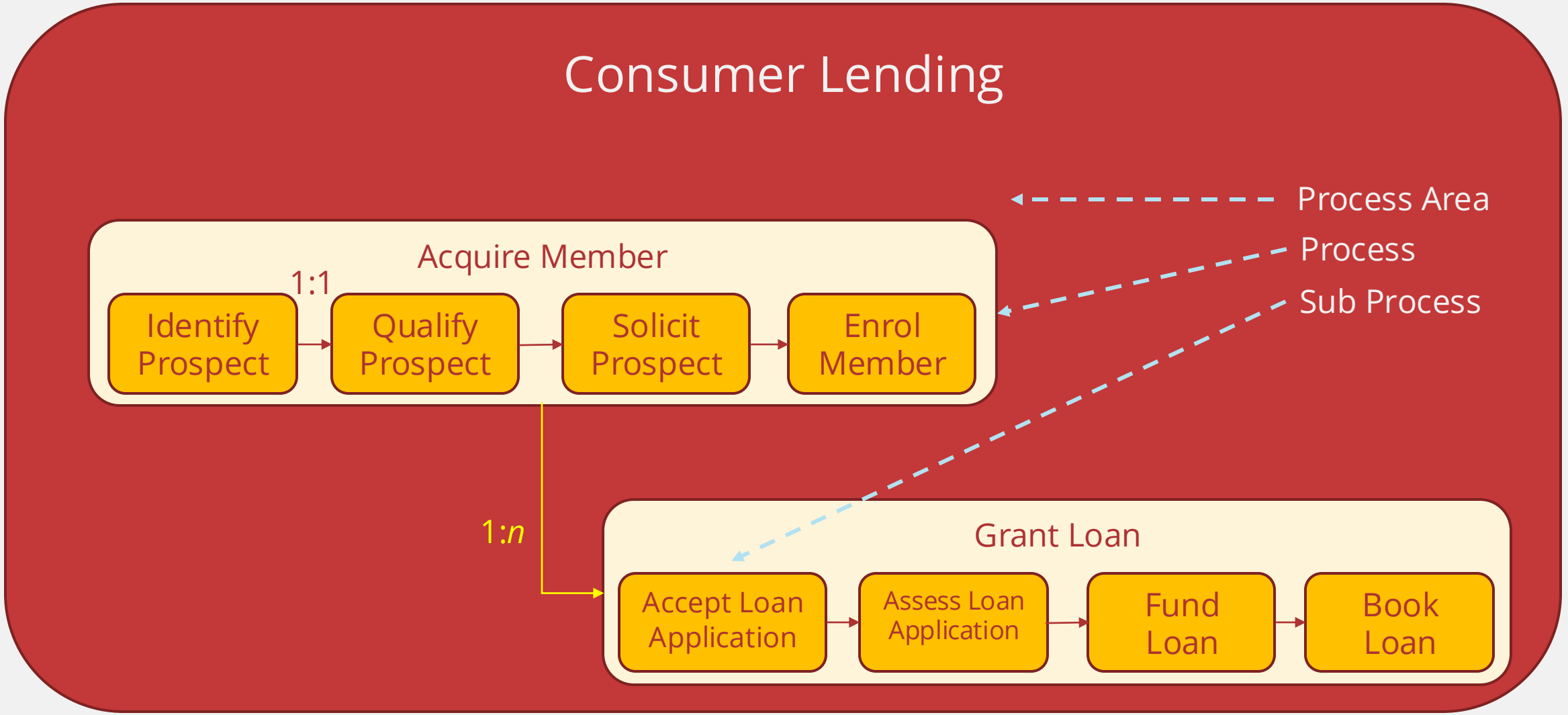
A thing is done…

…to a thing.

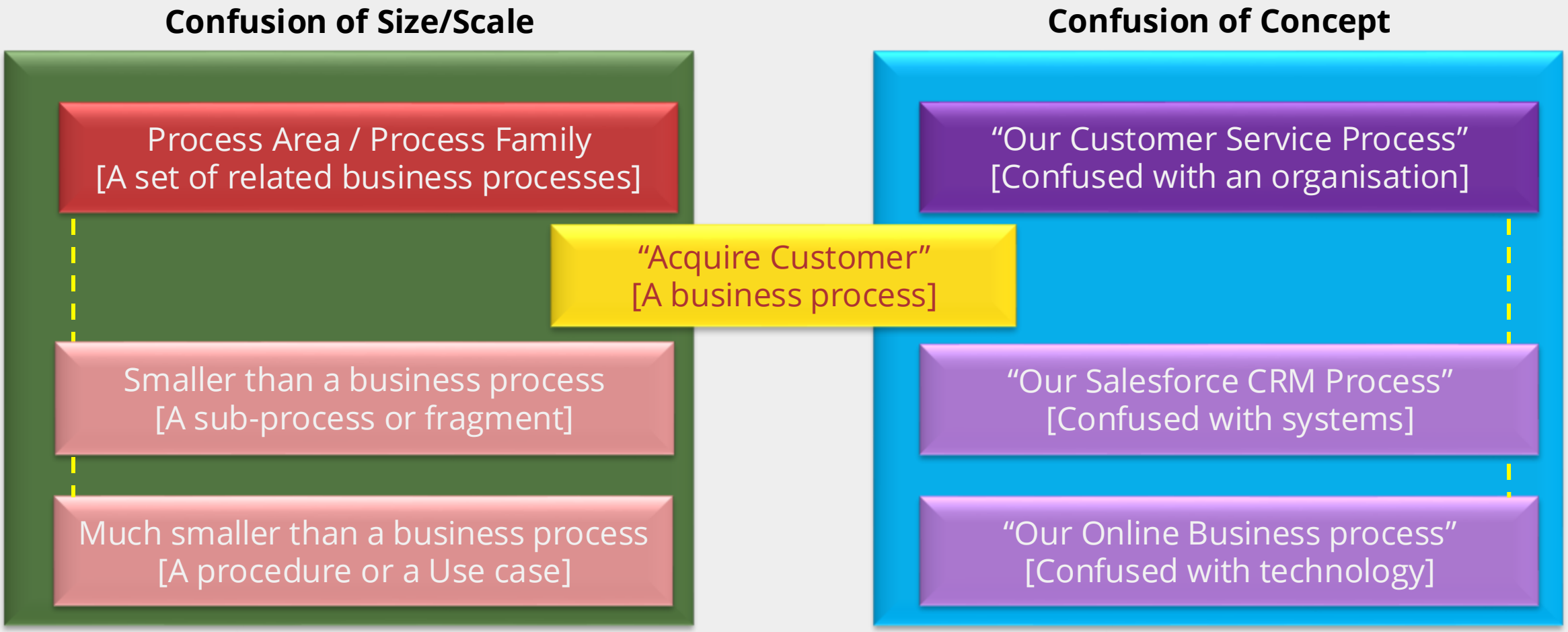
What is a Process?

- Goals for each function
- Applications used by each function
- Data required by each function
- Understand source for data in each function
- Technology required by each function

What is a Process?



What processing activities should you be documenting?



Exercise

- Think about the key functions in your organisation.
- Identify them by business function area (e.g. HR, Finance)
- Label them using Verb-Noun grammar
- Cluster them into related process groups
- Think about how you would probe for this information when interviewing / surveying your internal stakeholders

CASTLEBRIDGE

Module 5

Developing the ROPA: A Practical Architectural Approach

On completion of Module 5

nderstand	Understand the Zachman Framework and how an ARCHITECTURAL approach to ROPAS can help
Identify	Identify the common pitfalls with ROPA development and maintenance that this approach helps avoid
Explain	Explain the different tiers of risk that can be applied to support prioritisation of activities
Understand	Understand the need to capture completely across the Zachman Framework first

The Key Questions (again)

Zachman Framework for Enterprise Architecture

Horizontally, this encompasses all the questions in Article 30

	Data	Action	Location	Actor	Event	Motivation	
Executive	Inventory Identification	Process Identification	Distribution Identification	Responsibility Identification	Timing Identification	Motivation Identification	Scope & Context
Business Manager	Inventory Definition	Process Definition	Distribution Definition	Responsibility Definition	Timing Definition	Motivation Definition	Business Concepts
Architect	Inventory Representation	Process Representation	Distribution Representation	Responsibility Representation	Timing Representation	Motivation Representation	System Logic
Engineer	Inventory Specification	Process Specification	Distribution Specification	Responsibility Specification	Timing Specification	Motivation Specification	Technology Physics
Technician	Inventory Configuration	Process Configuration	Distribution Configuration	Responsibility Configuration	Timing Configuration	Motivation Configuration	Tool Components
Enterprise	Inventory Instantiation	Process Instantiation	Distribution Instantiation	Responsibility Instantiation	Timing Instantiation	Motivation Instantiation	Enterprise

Vertically: Captures the detail

The Zachman Perspectives and ROPA

Zachman Perspective	Stakeholder Representative	ROPA Contribution
Executive	Senior leaders, DPO, board	Process areas and organisational scope; high-level purposes; strategic data categories
Business Manager	Process owners, department heads	Named processing activities; legal bases; data subject categories; business rules
Architect	Information architects, data stewards	Data flows, lineage, system dependencies; categories of recipients; cross-border transfer mechanisms
Engineer	IT managers, system owners	System-level technical metadata; security controls; integration points; data formats
Technician	DBAs, developers, operations	Specific fields, retention enforcement mechanisms, access controls

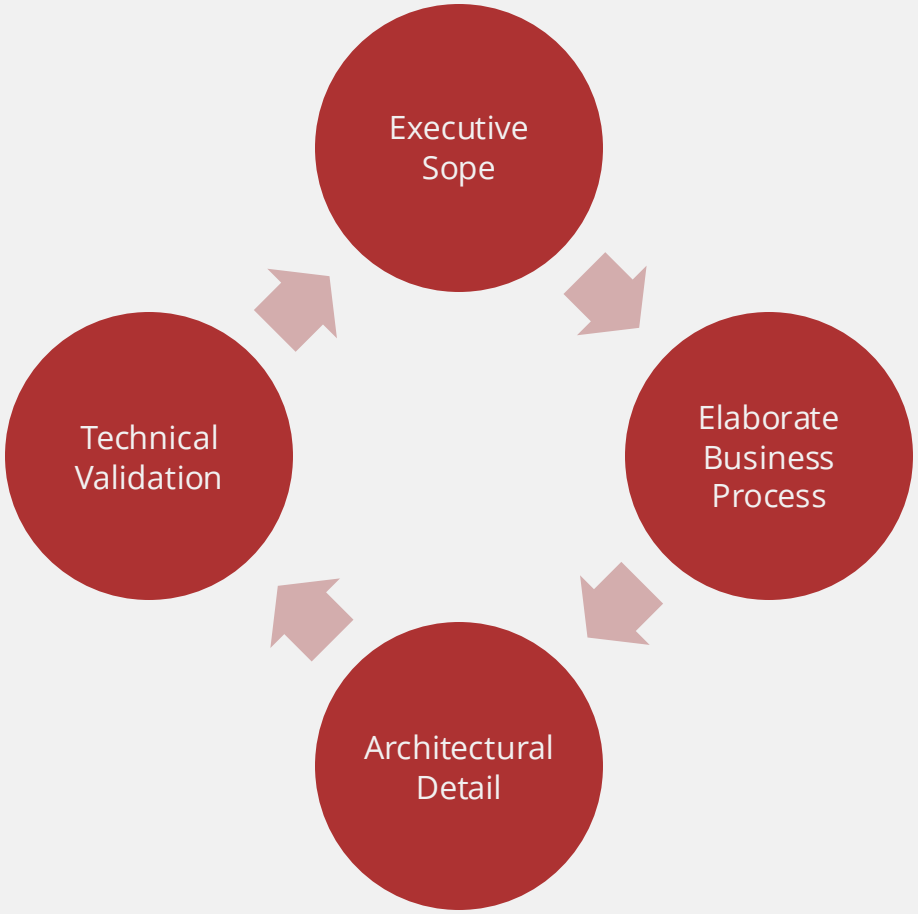
Definition of Good: Architecture Perspective

- Good =
  - A Complete description HORIZONTALLY of the METADATA
  - For the key business functions
  - Defined to an appropriate level of granularity
  - Proportionate to the risk, complexity, or nature of the processing
  - That has clearly assigned accountability for accuracy and timeliness
- Bad =
  - Granular detail
  - For a single process
  - That is incomplete
  - That lacks governance accountability

Granularity Driven by Risk

Tier 1 High Risk	Processing activities involving special category data (Article 9), large-scale processing, systematic monitoring, profiling with significant effects, or activities likely to require a DPIA. These require elaboration through all relevant Zachman perspectives. Engagement must extend from process owner through to technical stakeholders to ensure the ROPA entry is sufficiently detailed to support the associated DPIA and to identify the specific technical and organisational controls in place.
Tier 2 Standard Risk	Core operational processing activities involving ordinary personal data with clear, established legal bases. These require elaboration to the Architect level — sufficient to document data flows, recipients, and retention — but do not necessarily require deep technical metadata from engineer or technician perspectives.
Tier 3 Lower Risk	Routine, well-understood activities with minimal data subject impact, clear legal bases, and established controls. Documentation at the Executive and Business Manager levels is likely sufficient for initial ROPA development, with elaboration deferred unless the risk profile changes.

The Iterative Elaboration



- Executive Scope:
  - Define Organisational Boundary
  - Identify High Level Process Areas
  - Identify key risk tiers
  - Define high level categories of data subject / data
- Business Process Elaboration
  - Engage Business Function heads
  - Prioritise drilldown based on risk
  - Capture business function level metadata
  - Flag functions that may require DPIA, DP Agreements, LIAs, TIAs etc.
  - Baseline compliance for Article 30
- Architectural Detail
  - More detailed metadata for higher risk / higher value processes
  - Additional metadata such as system dependencies, data flows, and validation of source and recipient categories enriches ROPA and makes it a core **data governance** resource

Benefits of this Approach

- Avoids two failure modes in ROPA Development
  - **Shallow ROPA** – stuck at Executive or Business Function level without sufficient granularity or ability to function as a governance tool
  - **Paralysed ROPA** – ROPA activity swamped by attempt to capture granular detail resulting in document too complex to maintain and stakeholders who are overwhelmed.
- **Balance detail needed to level of risk**
- **Capture broad picture first and then drill down iteratively**
- **ROPA is a LIVING DOCUMENT**

Applying this to Engaging Stakeholders

1. Use Verb-Noun language to identify the Processing Activity at each level.
2. Iteratively drill down using open questions (“tell me about”, “describe for me”
3. Use the Zachman Framework as a set of ‘pigeon holes’ to track what you know at what level of abstraction
4. Living document is a critical concept
   - Business Functions need to be accountable for their ROPA entries
   - Business Functions should lead on elaborating the detail

CASTLEBRIDGE

Module 6

Categories & Categorisation of Data and Data Subjects

On completion of Module 6

Able to	Able to distinguish between categorisation of data and categorisation of data subjects as two distinct but related forms of business metadata
Identify	Identify the legal significance of data classification within the ROPA, including triggers created by processing of Article 9 or Article 10 data
Apply	Be able to apply a structured classification taxonomy to personal data within a processing activity at an appropriate level of abstraction
Explain	Be abl to explain how classification and categorisation function as business metadata when ROPA acts as metadata hub, highlighting linkage to DPIAs, Retention schedules etc.
Evaluate	Evaluate the governance implications of classification decisions, including how inconsistent categories undermine Article 15 requests, create gaps, and weak compliance under Article 5(2)

Categories of Subject vs Categories of Data

Categories of Data Subjects		Categories of Personal Data
Who is the data about?	≠	*What type of information?*
• Employees • Contractors and interns • Customers / clients • Job applicants • Suppliers' contacts • Former employees		• Contact details • Financial data (salary, bank details) • Health data (sick leave, occupational records) • Biometric data • Location data • Criminal convictions data (Art. 10)

Entity

Attribute

Key point: One data subject can have many categories of personal data. These are separate ROPA columns - never conflate them.

CASTLEBRIDGE

Good Practice from DPC

DPC Guidance Note (April 2023)

"Controllers could start with a common business function such as HR. This business function is likely to have several different purposes for processing, with each purpose involving different categories of individuals (for example employees, contractors and interns) and with each individual having several categories of personal data (such as health and safety information, sick leave, payroll details)."

DPC, Guidance Note, April 2023

Categories of personal data per data subject group:

Employees	Contractors	Interns
• Health & safety records • Sick leave records • Payroll details • Performance reviews	• Tax and invoicing data • Contract terms • Security access logs • Skills / qualifications	• Contact details • Emergency contacts • Training records • Attendance data

CASTLEBRIDGE

Special Category Data

Racial or ethnic origin	**Political opinions**	**Religious or philosophical beliefs**	**Trade union membership**
Genetic data	**Biometric data (for identification)**	**Health data**	**Sex life or sexual orientation**

Article 10 - Criminal convictions and offences: Governed separately from Article 9. Common Irish examples: Garda vetting, disclosure of prior offences. Equivalent restrictions apply.

Explicit legal basis required

An Article 9(2) condition must be identified and documented, in addition to the Article 6 lawful basis.

DPIA likely required

High-risk threshold is often met for special category processing. Classification triggers the DPIA assessment.

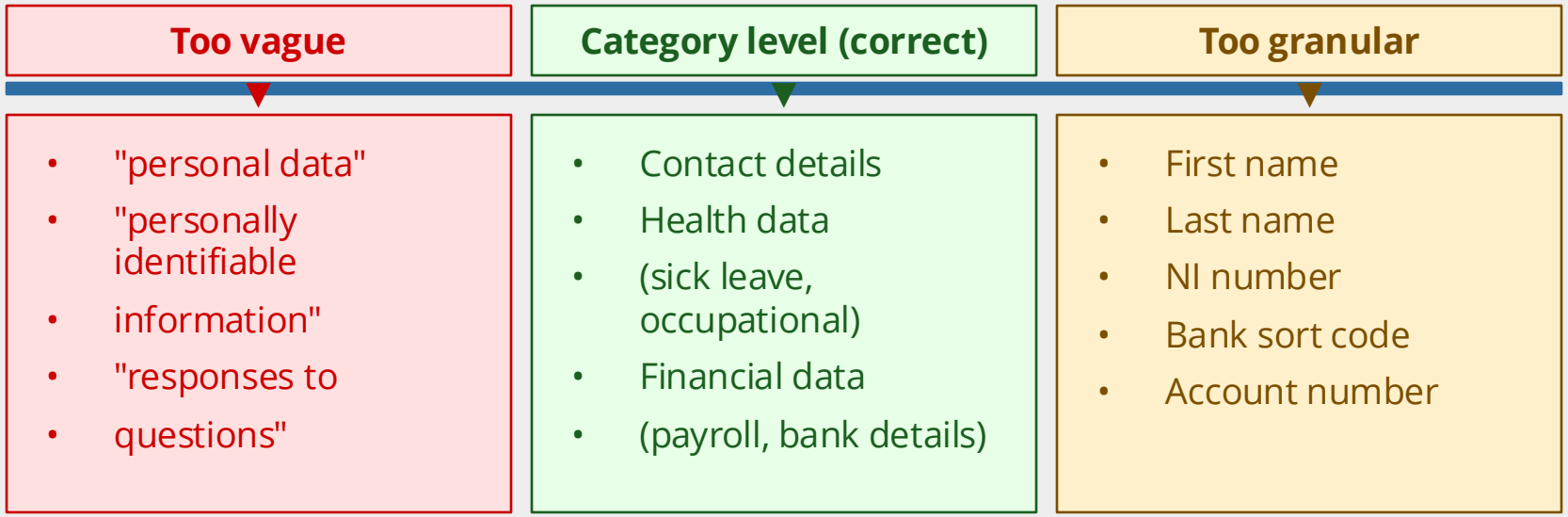
Enhanced controls needed

Security measures, access restrictions, and retention periods must reflect the heightened sensitivity of the data.

Has implications for quality / completeness of ROPA if categories of special category data are not identified

The Granularity Problem

DPC Sweep Finding - Insufficient Category Descriptions
Responses stating 'personal data', 'personally identifiable information' and 'responses to questions' were received. These are unequivocally not sufficient in describing what information is actually collected.
(DPC, April 2023)



Field-level detail is unmaintainable as systems change.

Key Principle

Classification and categorisation are not administrative checkbox fields. They are the foundational business metadata that determines legal obligations, risk profile, governance linkages, and the organisation's ability to demonstrate accountability under Article 5(2) GDPR.

The DPC has made clear: *a ROPA with insufficient detail is, in its view, no ROPA at all.*

Challenge in Organisations

CONSISTENCY OF CATEGORISATION

VERSION CONTROLLING OF CATEGORY METADATA

TRAINING AND UNDERSTANDING FOR STAFF IN METADATA

CASTLEBRIDGE

Module 7

Data Retention as Metadata: Practical Approaches

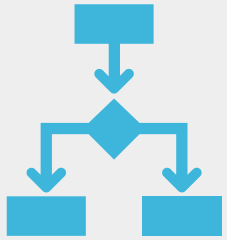
On completion of Module 7

Able to	Able to distinguish between a retention *rule* and a retention *trigger*
Understand	Understand that different processing activities may require the same data to be retained for different periods in identifiable forms
Identify	Identify common sources for retention rules for personal data
Define	Be able to define an actionable and enforceable retention rule using a Trigger / Rule / Action construct
Explain	Explain the relationship between a ROPA and a Retention Schedule

Data Retention and ROPA – MVP needed?

MVP = Nothing. (Retention only required “where possible”)

Implication: Red flag for a regulator



Resolution: Include something!

Rules vs Triggers

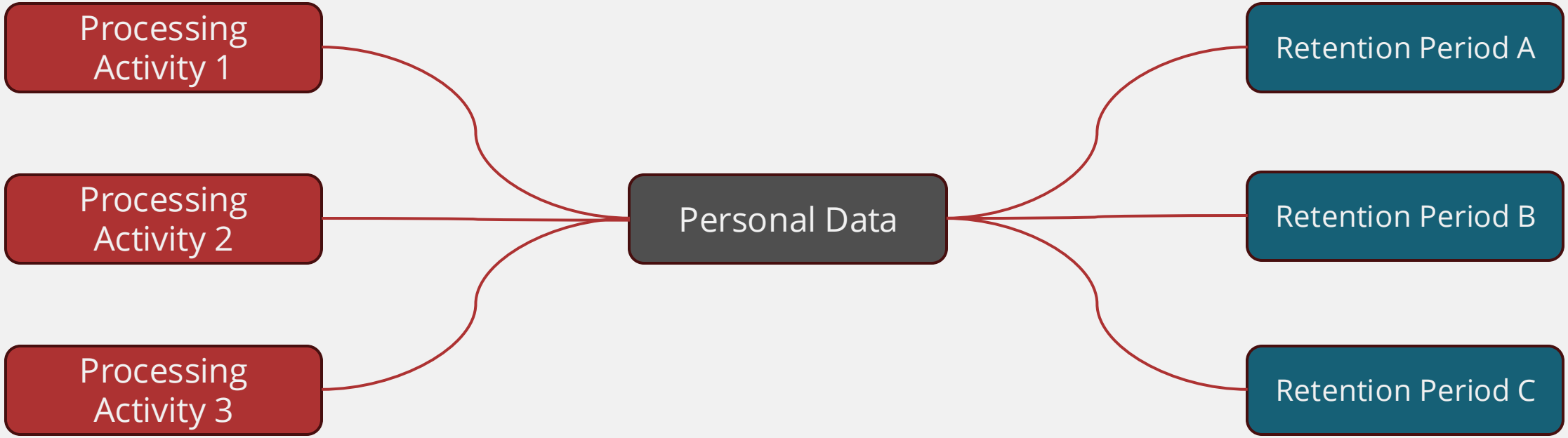
Rule

- Retain Customer Data for 6 years

Trigger

- Date of last purchase
- Expiry of warranty period
- Completion date of last project

Important: 1 Data Item can have >1 Retention Period

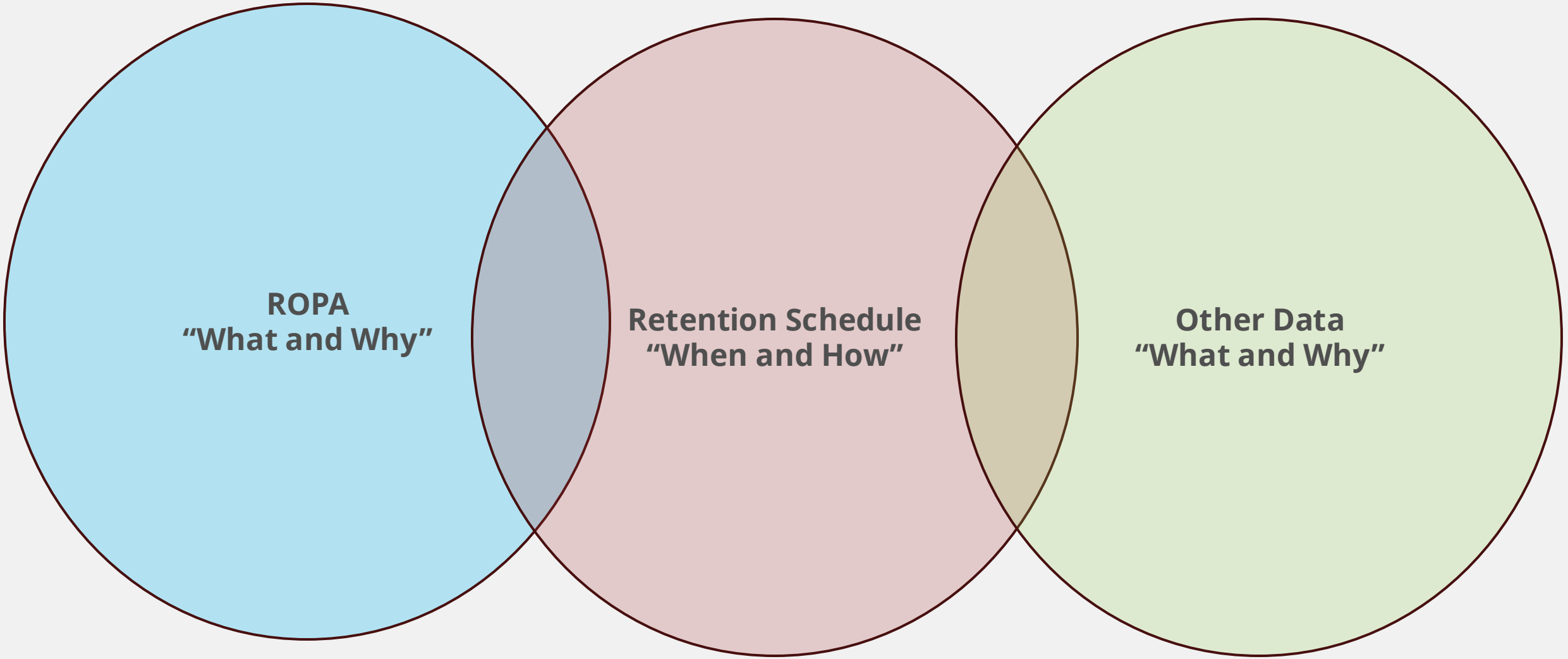


ROPA can identify this if there is consistent categorisation across Business Functions

Sources of Retention Rules

- If including in ROPA, include evidence / source / reason
- Common sources:
  - Statutory provision (usually a minimum period not a maximum)
  - Custom and practice in sector (need to ensure evidence of this)
  - Contractual requirement
  - Internal policy decision
- When defining the rule must ensure Trigger / Rule
- Trigger + Rule must result in ACTION

Relationship between ROPA and Retention Schedule



DPC Guidance

- If you are including Retention
  - ROPA must be self-contained
  - Links out to other documents must work
- Vague data categories like “HR Data” do not give sufficienty granularity
  - What HR Data?
    - Sick Leave
    - Disciplinary records
    - Training Records
    - Performance reviews

CASTLEBRIDGE

Module 8

ROPA, DPIA, and Other Governance Controls

On completion of Module 8

Explain	Explain the relationship between the ROPA and the DPIA, including how ROPA metadata functions as the trigger mechanism for Article 35 and why aa DPIA cannot substitute for the separate obligation to maintain a ROPA.
Identify	Identify the Article 35 criteria that indicate a DPIA is likely required, and describe how accurate ROPA metadata — covering categories of data, data subject groups, purposes, and recipients — provides the factual foundation for defensible scoping decisions.
Understand	Understand the governance linkages between the ROPA and other compliance instruments, including processor agreements (Article 28), privacy notices (Articles 13/14), security controls (Article 32), and transfer documentation (Chapter V), explaining how the ROPA functions as the connective register that keeps these instruments coherent and consistent.
Assess	Assess the downstream consequences of misalignment between the ROPA and related governance controls, including DPIAs scoped to the wrong activity, processor agreements that do not reflect actual data flows, and privacy notices that no longer accurately describe processing.
Apply	Apply the accountability principle under Article 5(2), demonstrating how a live, maintained ROPA provides the evidential thread supporting regulatory engagement, breach management, and data subject rights responses.

ROPA & DPIA

DPC, Guidance Note on RoPA (April 2023):

"The RoPA is a standalone record, a compliance tool that the DPC should be able to rely on to provide an accurate view of data processing taking place within an organisation. Not every processing activity would have, or require, a DPIA."

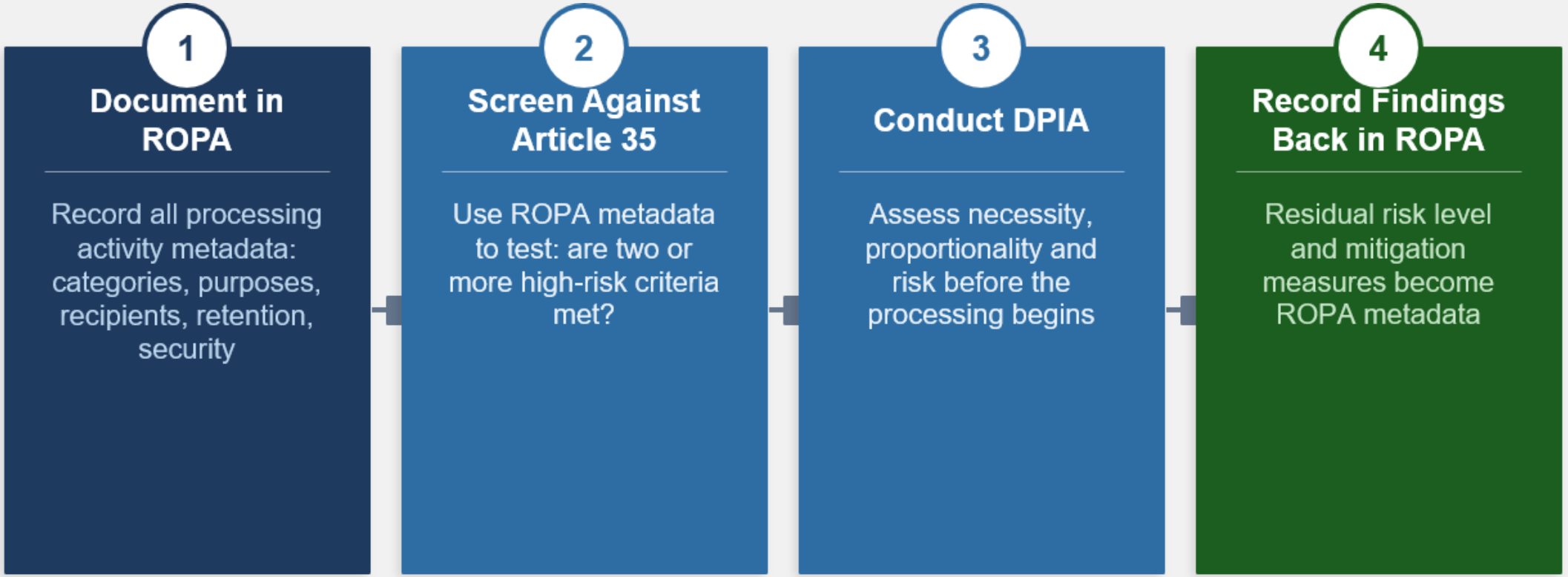
ROPA

- Continuous Obligation
- Applies to all processing activities
- Must be maintained in writing
- Must be available to DPC on request
- Records activities that use personal data

DPIA

- Completed before processing begins
- Applies only to high-risk processing
- Assesses necessity proportionality, risk
- Review required when risk profile changes
- Not a substitute for ROPA

How ROPA and DPIA work together



Feedback loop: DPIA findings (residual risk level and mitigation measures) are recorded back into the ROPA entry for that processing activity

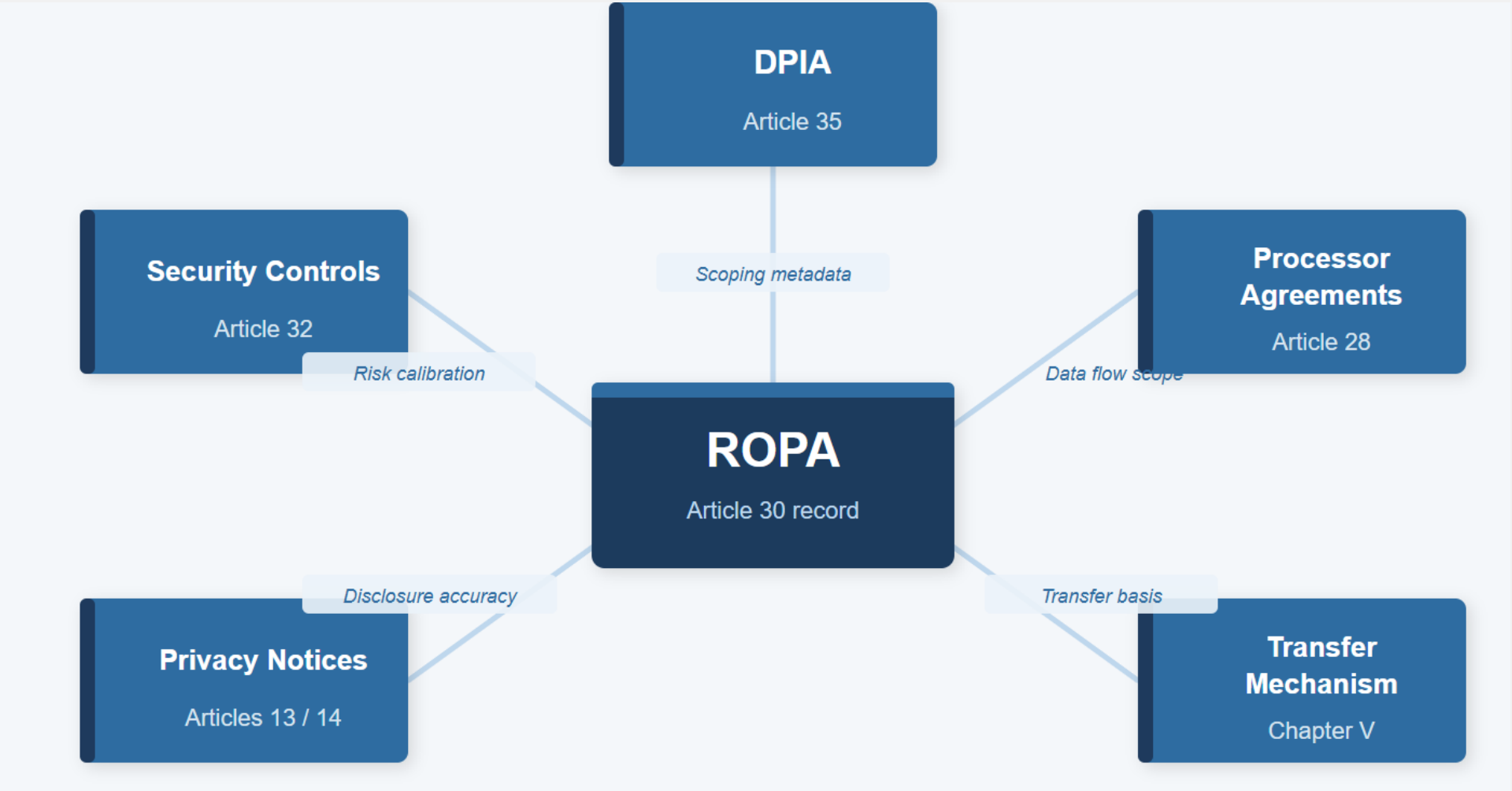
CASTLEBRIDGE

ROPA Metadata and DPIA Scoping

Each Article 35 criterion maps directly to a ROPA field

ROPA Field	Article 35 Criterion	What It Checks	Risk of Vagueness
Categories of personal data	Criterion 4 — Sensitive data	Are Article 9 categories involved? Is Art.35(3)(b) triggered?	*"Personal data" masks sensitivity; DPIA missed*
Purpose of processing	Criterion 1 — Profiling / Criterion 2 — Automated decisions	Does the activity involve scoring, profiling, or automated outcomes?	*"Marketing" hides profiling; criterion not applied*
Categories of data subjects	Criterion 7 — Vulnerable individuals	Are children, patients, or employees affected?	*"Customers" misses children or vulnerable groups*
Recipients and transfers	Criterion 9 / Chapter V risk	Does processing enable or block access to a service or right?	*Third-country transfer undisclosed; no SCCs in place*

ROPA as Connective Tissue



Implications of Defective ROPA

An outdated ROPA causes downstream failures across the entire governance framework

⚠ DPIA

DPIA Scoped to the Wrong Activity

If the ROPA has not been updated to reflect a change in processing, the DPIA assesses the risk of a version of the activity that no longer exists.

Art. 35(11): DPIA must be reviewed when the risk profile changes.

⚠ Art. 28

Processor Agreement Gaps

New data categories or purposes not reflected in the ROPA will also be missing from the Article 28 agreement — leaving processing outside the contractual scope.

Processors handling data beyond agreed scope = direct enforcement risk.

⚠ Art. 13/14

Privacy Notice Inaccuracies

Purposes, retention periods, and recipients in the ROPA must match those disclosed to data subjects. Misalignment is a transparency failure under Articles 13–14.

Breach notification context: affected data subjects may have been misinformed.

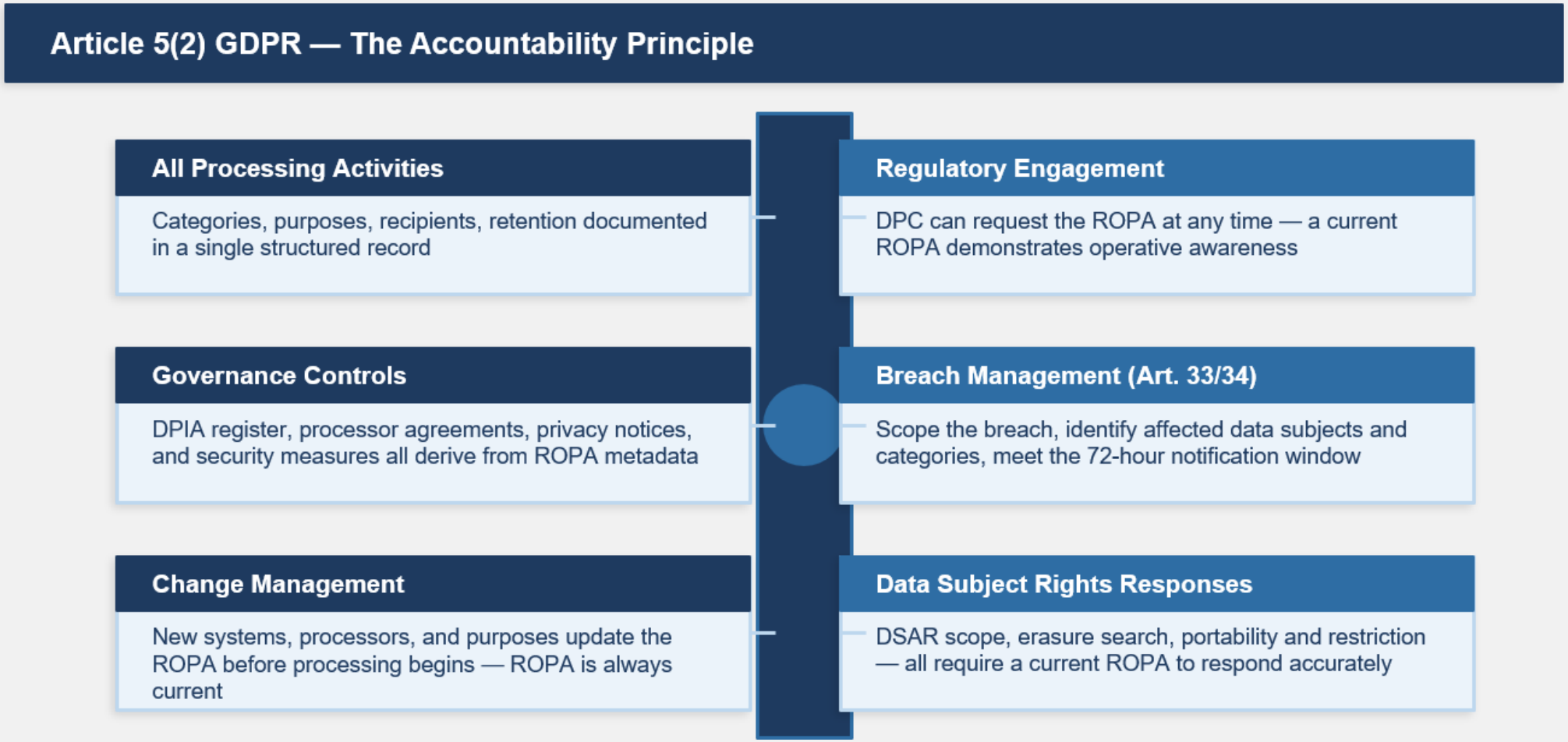
⚠ Art. 33

Breach Response Compromised

Under Article 33 organisations have 72 hours to notify the DPC of a breach, including categories and approximate numbers affected. An inaccurate ROPA makes this impossible to scope reliably.

DPC can request the ROPA at any point, including during breach management.

Connecting ROPA to Accountability Credibility



CASTLEBRIDGE

Key Principle

ROPA is single source of truth for metadata that describes the processing of personal data in the organisation

CASTLEBRIDGE

Module 9

ROPA’s Role in NIS2, EU AI Act, and other regulatory requirements

On completion of Module 9

Explain	Explain how ROPA can help support NIS2 compliance
Understand	Understand the importance of reflecting AI / GenAI use in ROPAs to support EU AI Act risk assessment
Understand	Understand limitations of ROPA in wider regulatory landscape

ROPA and NIS2

- Robust ROPA supports NIS2 compliance
- Focus on process activity and data in business function context key
- Risk-based perspective key
- *BUSINESS FUNCTION HEAD / EXEC level liability also key!*
- Both obligations are expressions of the same underlying governance requirement: **know your information assets, understand the risks to them, and be able to demonstrate you've managed those risks appropriately**
- **What are you securing when you secure data and processes under NIS2?**

ROPA NIS2 Intersection 1

Asset Identification and Inventory

- The ROPA records the systems, processes, and data flows involved in personal data processing. This maps directly onto the NIS2 requirement for asset management (Article 21(2)(i) in the implementing framework). A well-structured ROPA — one that records systems and not just processing purposes — provides the foundation for the NIS2 asset inventory rather than requiring a separate exercise.
- The practical gap is that the ROPA is scoped to personal data while NIS2 applies to *all* network and information systems. But where systems process personal data (which for most essential and important entities is most of them), the ROPA is doing much of the heavy lifting.

ROPA & NIS2 Intersection 2

Security Measures Documentation

- Article 30(1)(g) requires controllers to record "where possible, a general description of the technical and organisational security measures referred to in Article 32." This is the explicit GDPR bridge to security. NIS2 Article 21 specifies a minimum set of those measures — risk analysis, access control, cryptography, incident handling, supply chain security, etc.
- The implication: the security measures column of your ROPA *should* be populated with reference to your NIS2 Article 21 controls. If it isn't, you have a gap in both your GDPR and NIS2 documentation. Many ROPAs leave this field thin or generic ("appropriate technical and organisational measures"), which satisfies neither obligation.

ROPA & NIS2 Intersection 3

Supply Chain and 3rd Party Mapping

- Article 30(1)(d) requires recording recipients of personal data, including processors. Article 30(2) requires processors to maintain their own records referencing the controllers on whose behalf they act. This gives you a map of your data supply chain.
- NIS2 Article 21(2)(d) requires supply chain security — understanding the cybersecurity posture of suppliers and service providers.
- Your Article 30 processor register is your starting point for NIS2 supply chain risk assessment. The ROPA tells you who your third parties are and what data they handle; NIS2 due diligence then requires you to assess their security controls.

ROPA & NIS2 Intersection 4

Incident Response Scoping

- When a cybersecurity incident occurs, a key immediate question is: *does this constitute a personal data breach?* The ROPA answers that question. It tells you which processing activities are hosted on affected systems, which categories of personal data are at risk, and which data subjects are potentially affected — all of which determines whether GDPR Article 33 (72-hour supervisory authority notification) and Article 34 (data subject notification) are triggered alongside NIS2 Article 23 obligations.
- NIS2 Article 23 requires an early warning within 24 hours of a significant incident, a formal notification within 72 hours, and a final report within one month. For incidents involving personal data, these timelines run concurrently with GDPR breach notification. The ROPA is the operational reference document for scoping the breach.

ROPA & NIS2 Intersection 5

Risk Assessment Integration

- GDPR requires a risk-based approach to security (Article 32), and the DPIA process (Article 35) for high-risk processing. NIS2 requires formal risk analysis of network and information systems. These should be integrated — the same risk assessment methodology should feed both the DPIA/Article 32 analysis and the NIS2 risk management framework.
- In practice this means the risk register feeding your Article 30 security measures documentation and your NIS2 Article 21 risk analysis should be the *same risk register*, not two separate exercises with inconsistent risk ratings for the same systems.

Divergences to watch

Availability and resilience are NIS2 Article 21 requirements (business continuity, backup management, crisis management) that have no direct home in the ROPA structure, which is primarily a confidentiality and accountability instrument.

Non-personal data processed on the same systems is invisible to the ROPA but fully in scope for NIS2.

Operational technology (OT) systems in energy, transport, and water entities may have minimal personal data processing but significant NIS2 obligations — the ROPA contributes little there.

Practical Steps

- **Use the ROPA as the foundation** of your information asset management, but extend it — add fields for system criticality, availability requirements, and resilience classification.
- **Consolidate your security controls documentation** so that Article 32/ROPA and NIS2 Article 21 are drawing from the same controls framework (ISO 27001 or equivalent).
- **Integrate your processor/supplier register** into a single supply chain risk management process serving both Article 28/30 GDPR and NIS2 Article 21(2)(d).
- **Align incident response procedures** so the GDPR breach assessment and NIS2 incident classification happen in the same workflow, not parallel ones with potentially inconsistent conclusions.

ROPA and EU AI Act

- ROPA obligation is deepened not replaced.
  - Both instruments share a common underlying logic: **accountability through documentation, risk stratification, and demonstrable control**. But they approach the same organisational reality from different angles:
  - The **ROPA** asks: *what personal data are you processing, for what purpose, with what safeguards?*
  - The **EU AI Act** asks: *what AI systems are you deploying, at what risk level, with what controls and for what intended purpose?*

Five Key Intersection Points

1

AI System as Processing Activity

Each AI-enabled process needs a dedicated ROPA entry — not just the business function. Include an automated decision-making flag (Art. 22), cross-reference to AI system technical documentation, and output data recorded as a data category.

2

Training Data & Data Governance

Where personal data is used for AI training, it requires a separate ROPA entry with its own purpose, legal basis, and retention period. Annotation and labelling processors must be recorded under Art. 30 and Art. 10 AI Act.

3

Log Retention Alignment

Art. 26(6) mandates minimum 6-month log retention. Where AI system logs contain personal data, the ROPA entry must record this retention with Art. 6(1)(c) as legal basis — compliance with a legal obligation.

4

Special Category Data

Most Annex III high-risk use cases involve Art. 9 GDPR special categories (biometric, health, criminal). ROPA must record the Art. 9(2) legal basis, safeguards, and any Art. 10(5) bias-detection processing entries.

5

Provider / Deployer Role Mapping

AI Act roles (provider, deployer) don't map cleanly to GDPR roles (controller, processor). The ROPA's processor register is the operational foundation for AI Act Art. 25 supply chain obligations — but the logic runs in both directions.

Gaps – ROPA & AI Act

- **Lifecycle blindness.** The ROPA describes a processing activity as a relatively stable thing. The AI Act cares about an AI system's *full lifecycle* — design, development, training, validation, testing, deployment, monitoring, modification, decommissioning. The ROPA has no lifecycle dimension. A system that changes substantially after training (model drift, retraining on new data, significant modification under Article 3(23)) may require a new conformity assessment under the AI Act, but the ROPA will show no change unless someone actively updates it.
- **Non-personal training data.** The ROPA covers only personal data. AI training datasets frequently include substantial non-personal data (synthetic data, licensed datasets, publicly scraped content). The data governance obligations under Article 10 apply to all training data, not just personal data. The ROPA therefore gives an incomplete picture of the AI data governance position.
- **Intended purpose specificity.** The AI Act's concept of "intended purpose" (Article 3(12)) is more granular than a GDPR processing purpose. It includes the specific category of users, the deployment context, and foreseeable conditions of use. ROPA purpose entries are typically broader. This creates a risk of misalignment between what the ROPA says the system is for and what the technical documentation says — a problem in any regulatory examination that considers both documents together.
- **Post-market monitoring.** Article 72 EU AI Act requires providers to establish post-market monitoring plans with metrics and timelines. Where that monitoring involves processing personal data (e.g., feedback on AI outputs linked to identifiable individuals), new ROPA entries are required. Most post-market monitoring processing activities are currently undocumented in ROPAs because the obligation is new and the linkage hasn't been made.

ROPA Action plan for EU AI Act

1. **Extend the ROPA entry schema** for AI-enabled processing activities to include: AI system reference (cross-linked to technical documentation), risk classification (prohibited / high-risk / limited risk / minimal risk), intended purpose in AI Act terms, automated decision-making flag, and EU database registration number where applicable.
2. **Create dedicated ROPA entries for training data processing** — not just the downstream deployment. Training, validation, and post-market monitoring are distinct processing activities with different purposes, retention periods, and legal bases.
3. **Align log retention** in ROPA entries for AI system-generated logs with the Article 26(6) minimum, with the Article 6(1)(c) legal basis documented.
4. **Use the ROPA as the DPIA trigger mechanism** for AI deployments — the ROPA entry for an AI-enabled processing activity should be the document that initiates DPIA screening and, where Article 26(7) applies, flags the FRIA requirement.
5. **Map GDPR roles to AI Act roles** explicitly in the processor register — for each AI system provider recorded as a processor or supplier, document whether they are also an AI Act provider, and what conformity documentation has been received.

CASTLEBRIDGE

Module 10

Accountability, Governance, and the Role of the DPO in ROPA

On completion of Module 10

Able to	Able to explain the role of DPO in ROPA
Understand	Understand the role of business function heads in developing and maintaining ROPAs
Explain	Explain how effective data governance structures and behaviours are important to the maintenance of ROPAS
Understand	Understand the importance of structured reviews of ROPAs for accuracy and alignment to ACTUAL practices in the organisation

What is the role of the DPO re ROPA?

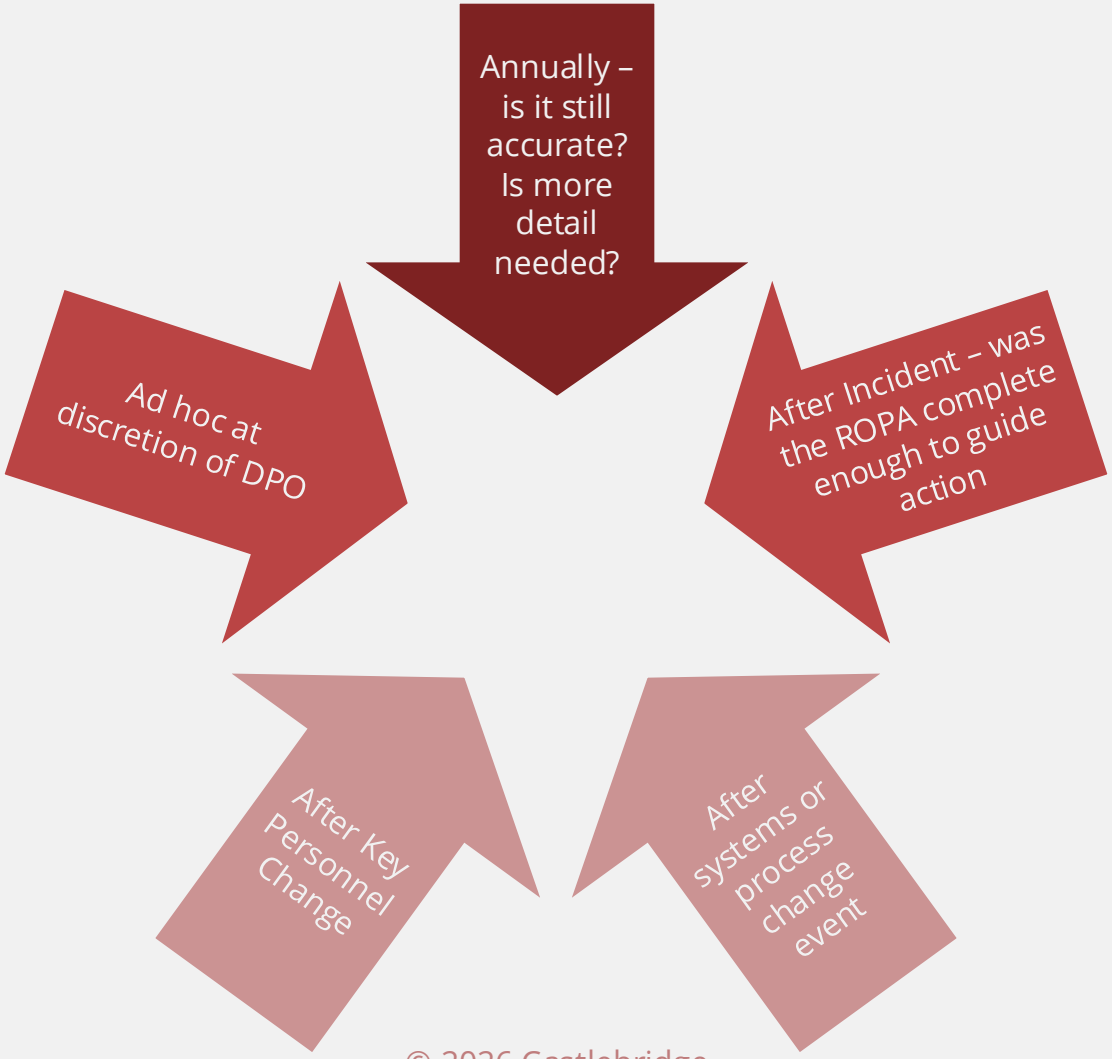
DPO Role re ROPA is…

- Ensure that it is being done
- Provide template for doing it
- Provide training on how to do it
- Provide guidance to stakeholders on how to do it
- Monitor that it has been done
- Quality Assure that it has been done right
- Escalate to senior management if it is not being done
- Consult with DPC under Article 39 if things aren't getting done

Governance = Behaviour of Situated Actors

- Business Function Heads are accountable for the documentation of their function
- ROPA is another element of their function to be documented.
- They are the closest to the ‘day to day’ to know what has changed or remained same
- Formal assignment of accountability is an appropriate Organisational Measure under Article 24
- Good Governance requires actual sanctions and supports to drive behaviour

Review of ROPA: When?



Review of ROPA: Why?

- Living Document
- Things change
- Risk (or risk appetite) changes
- Good practice

Presenting the ROPA to DPC

It needs to be “good to go” and instantly accessible

- As part of incident response
- On request from DPC
- On request from DPO (to business areas)

Governance of ROPA must therefore be supported by appropriate processes (and technology)

- Version control
- Publication approval

Must be a “self-contained” document

- Any links out to other documents need to work **outside** your environment
- Implication: If the information is not MANDATORY, omit from ROPA
- Implication: Formal ROPA may need to be a sub-set of a larger governance artefact

CASTLEBRIDGE

Article 30 and Human Factors

Enablers of Article 30 In Practice

- **Business Process Design:** The steps, decisions, sequence, and handoffs that constitute the workflow itself.
- **Information Systems/Technology:** The systems and tools that support the process.
- **Motivation and Measurement:** How performance is measured and rewarded. What metrics are used? What behaviours do those metrics encourage?
- **Human Resources and Organisation:** How roles and jobs are defined, how people are allocated to work. Are responsibilities clear?
- **Policies and Rules:** Internal policies, procedures, and the interpretation of external regulations.
- **Facilities:** The physical or digital workspace in which work occurs.

CASTLEBRIDGE

Enablers and ROPA Success

- **Motivation and Measurement:**
  - If business units are measured on operational efficiency but not on data protection compliance, ROPA maintenance will be deprioritised. If there is no recognition for good data stewardship and no consequence for poor documentation, ROPAs will become stale and incomplete.
- **Human Resources and Organisation:**
  - ROPA maintenance requires clear role definition. Who is responsible for documenting each processing activity? Who validates that documentation? Who ensures updates when processes change?
- **Policies and Rules:**
  - Interpretation of Article 30 requirements varies significantly across organisations. Some interpret "categories of personal data" broadly ("customer data"), others granularly. Without clear internal standards, different parts of the organisation will document at different levels of detail.

Dealing with Hidden Information Factories

The Hidden Information Factories

Examples

- Excel spreadsheet extracts and reports
- Local copies of data
- Notebooks with customer contact information
- Microsoft Access databases
- “Sandbox” IT systems

Action

- Record that they exist
- Log the risks that they are there
- Look to eliminate them over time
  - New systems
  - Improved controls etc.

Hidden Information Factories & Emergent Governance

- Hidden Information Factories are a outcome not a symptom
- Hidden data factories are an *inevitable product* of situated agents exercising practical reasoning based on their traditions and local knowledge.
- Addressing them means need into identify and record them and then determine the optimum approach to integrating or replacing them as part of ROPA development and data protection risk management improvement.

CASTLEBRIDGE

CASTLEBRIDGE

Wrap Up & Conclusion

CASTLEBRIDGE

What have we learned?

CASTLEBRIDGE

Extending the ROPA

CASTLEBRIDGE

Next Steps / Homework