PROGRAM MATERIALS
Program #2816
April 3, 2018

Complying with the EU General Data Protection Regulation (GDPR): Conducting Data Inventories

Celesq® AttorneysEd Center
www.celesq.com

5301 North Federal Highway, Suite 180, Boca Raton, FL 33487
Phone 561-241-1919 Fax 561-241-1969

Complying With the GDPR

Bryan Cave Data Privacy and Security Team

Agenda

Overview: GDPR

Module 1. Conducting Data Inventories

Module 2. Data Subject Requests

Module 3. Incident Response Plans

Module 4. Third Party Vendor Management Programs

Module 5. Cross Border Transfers

Module 6. Information Notices / Privacy Policies

Overview

BRYAN CAVE

Overview: Historical background

- The EU Data Protection Directive (EC/46/95)
  - Enacted in 1995
  - Creates a standard legal *framework* for EU member states.
  - It was not a self-implemented statute, regulation, or rule.
  - In US legal parlance, it was akin to an unfunded federal mandate.
  - There were 28 state implementing statutes in various languages, with various texts, and with various requirements.
  - There is an advisory body (the Article 29 Working Party) that provided interpretative guidance.

Overview: GDPR

The General Data Protection Regulation (EU) 2016/679

- Replaces the EU Data Protection Directive.
- Enters into force on May 2016,
- Applies beginning May 2018,
- Directly applicable in all EU Member States,
- Aims to unify data protection law within the European Union and increases data subject's rights,
- Still authorizes individual EU Member States to implement more specific rules in certain areas.

Overview: GDPR

The Countdown

BRYAN CAVE

Overview: GDPR 10 Top Talked About Provisions

1. Penalties. Under Directive functionally non-existent; under Directive up to 4% of revenue.
2. Floor not ceiling. Member states can enact additional safeguards in certain areas, including research.
3. Extraterritorial. Purports to impact "establishments" in the EU and other organizations that monitor behavior of EU data subjects or offer services to EU data subjects
4. Breach Notification. Adopts new breach notification obligations.
5. Children. Adopts US-like protections concerning collection of data from children.
6. Right to be Forgotten. Grants data subjects a right to have their information erased.
7. Right to Data Portability. Grants data subjects a right to ask for their information.
8. Data Protection Officers. Requires some organizations to designate data protection officers.
9. Data Privacy Impact Assessments. Requires organizations to create internal records concerning impact of high-risk processing.
10. Data Minimization. Requires that personal data be kept for no longer than is necessary.

BRYAN CAVE

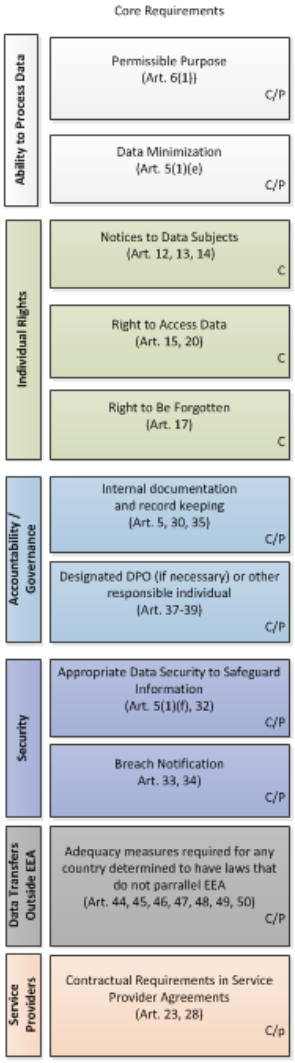
Overview: Core Requirements

Requirements differ depending upon whether you are a "Data Controller" or a "Data Processor."

- A "Data Controller" is defined as the entity which "determines the purposes and means of the processing of personal data." GDPR, Art. 4(7).

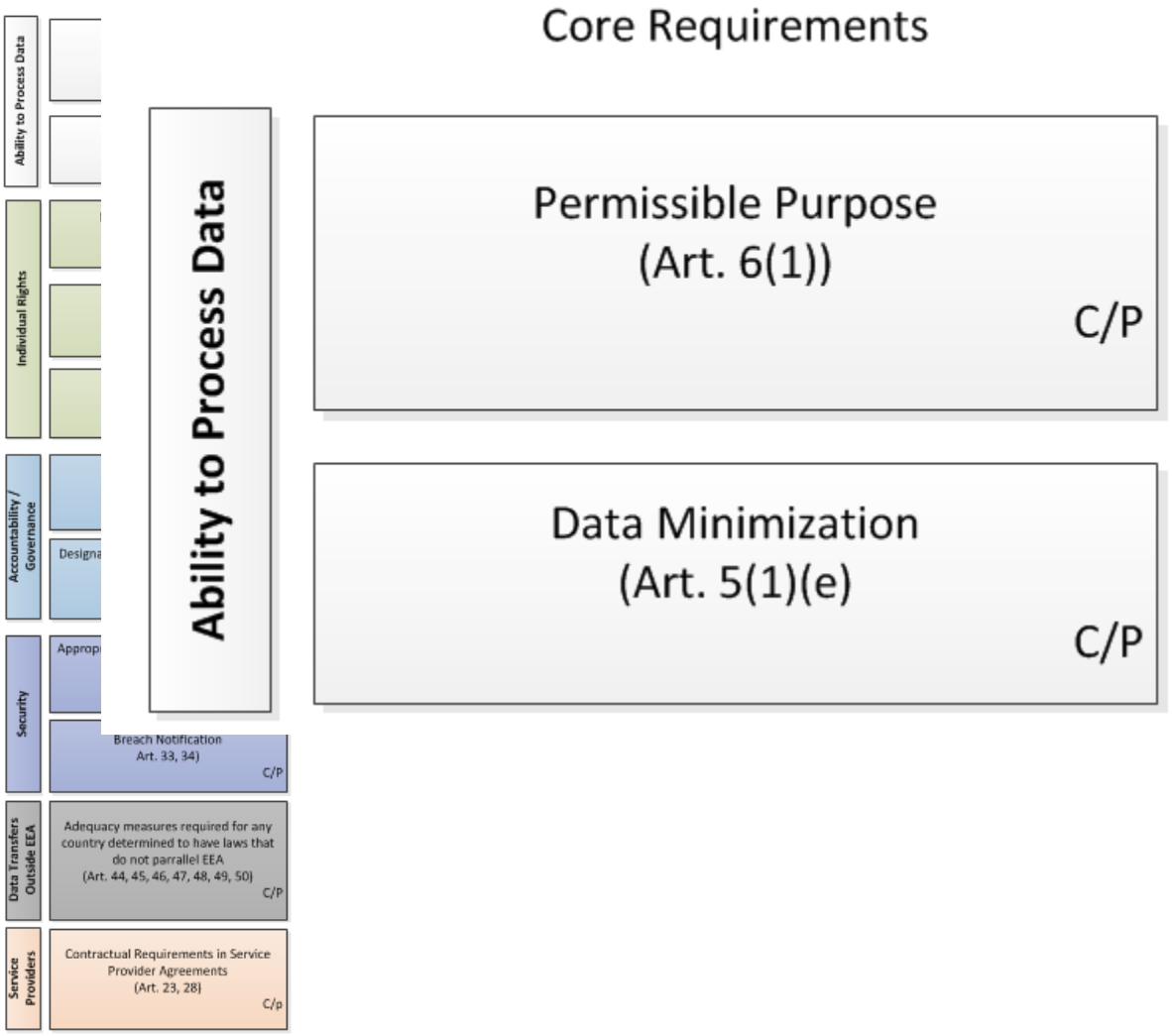
- A "Data Processor" is defined as an entity "which processes personal data on behalf of the controller." GDPR, Art. 4(8).

Overview: Core Requirements



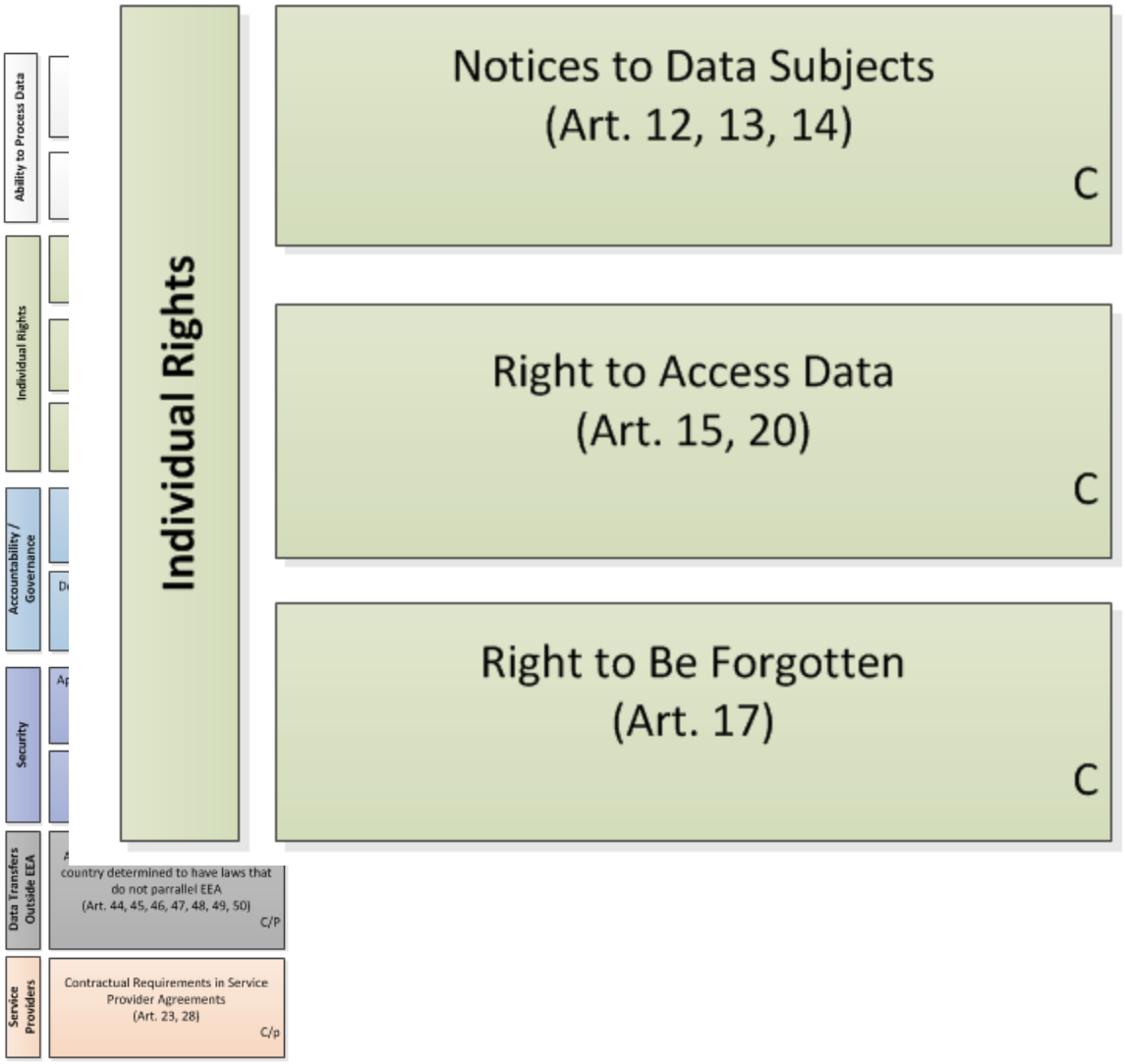
BRYAN CAVE

Overview: Ability to Process Data



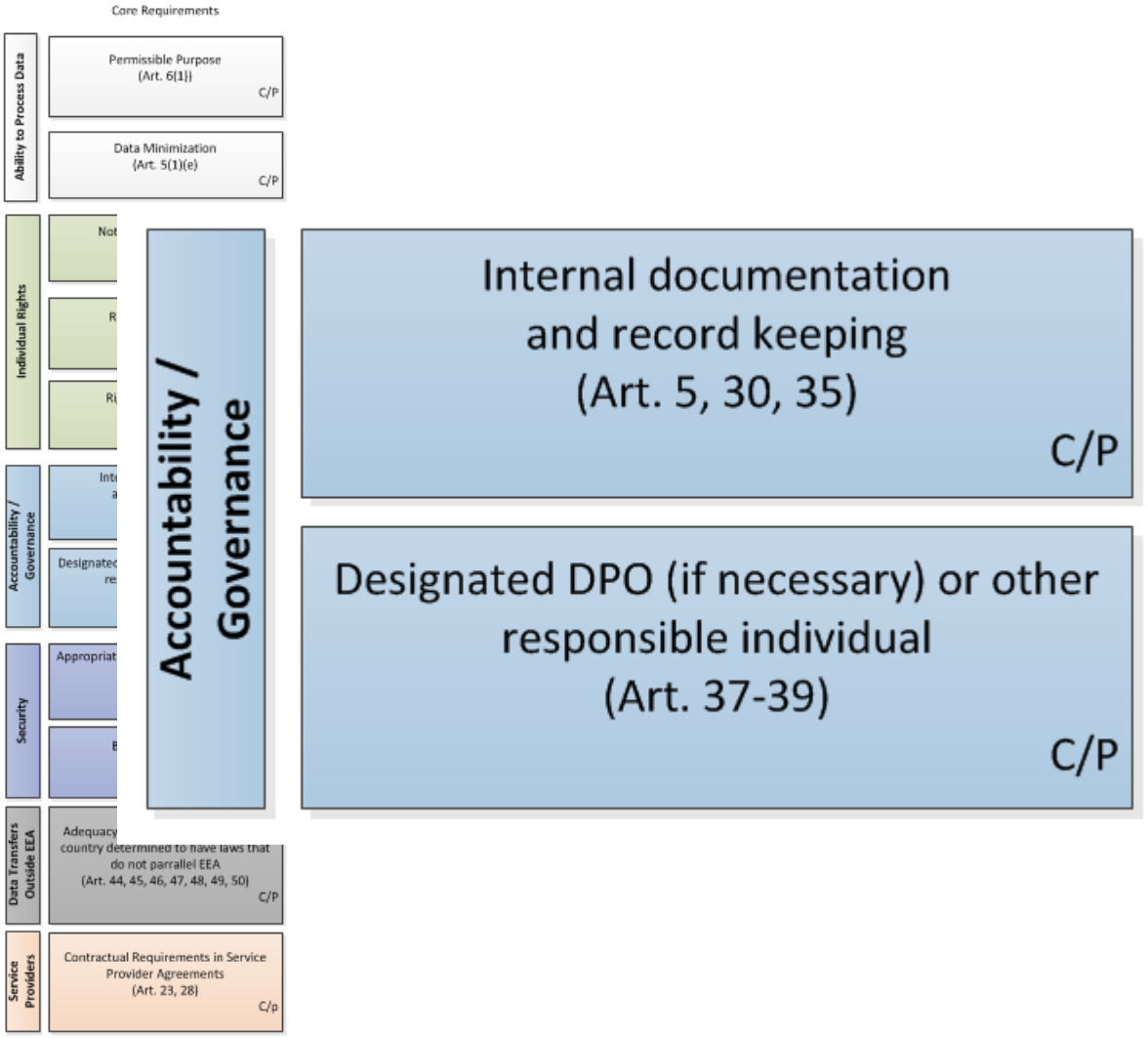
BRYAN CAVE

Overview: Individual Rights

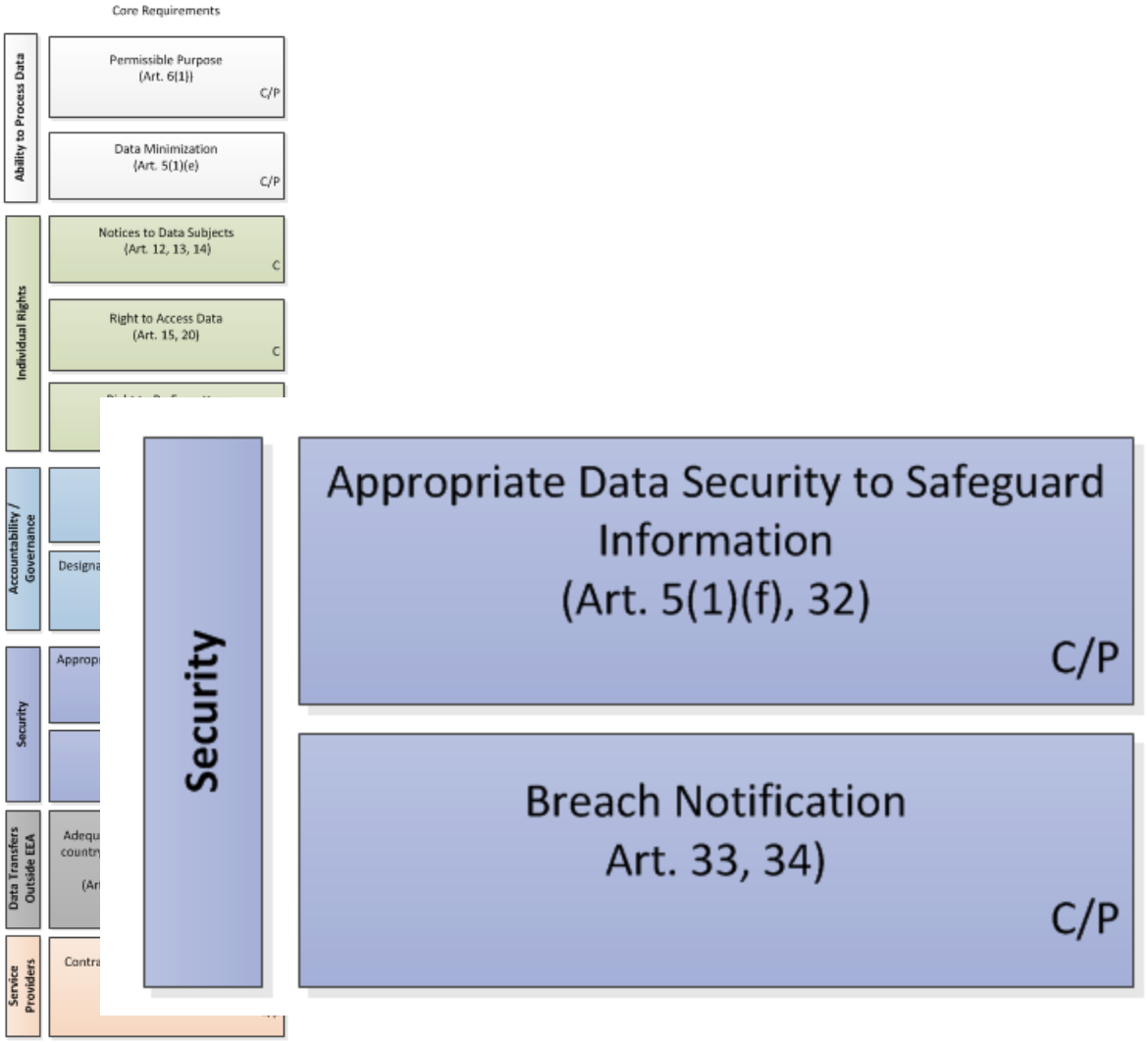


BRYAN CAVE

Overview: Accountability / Governance

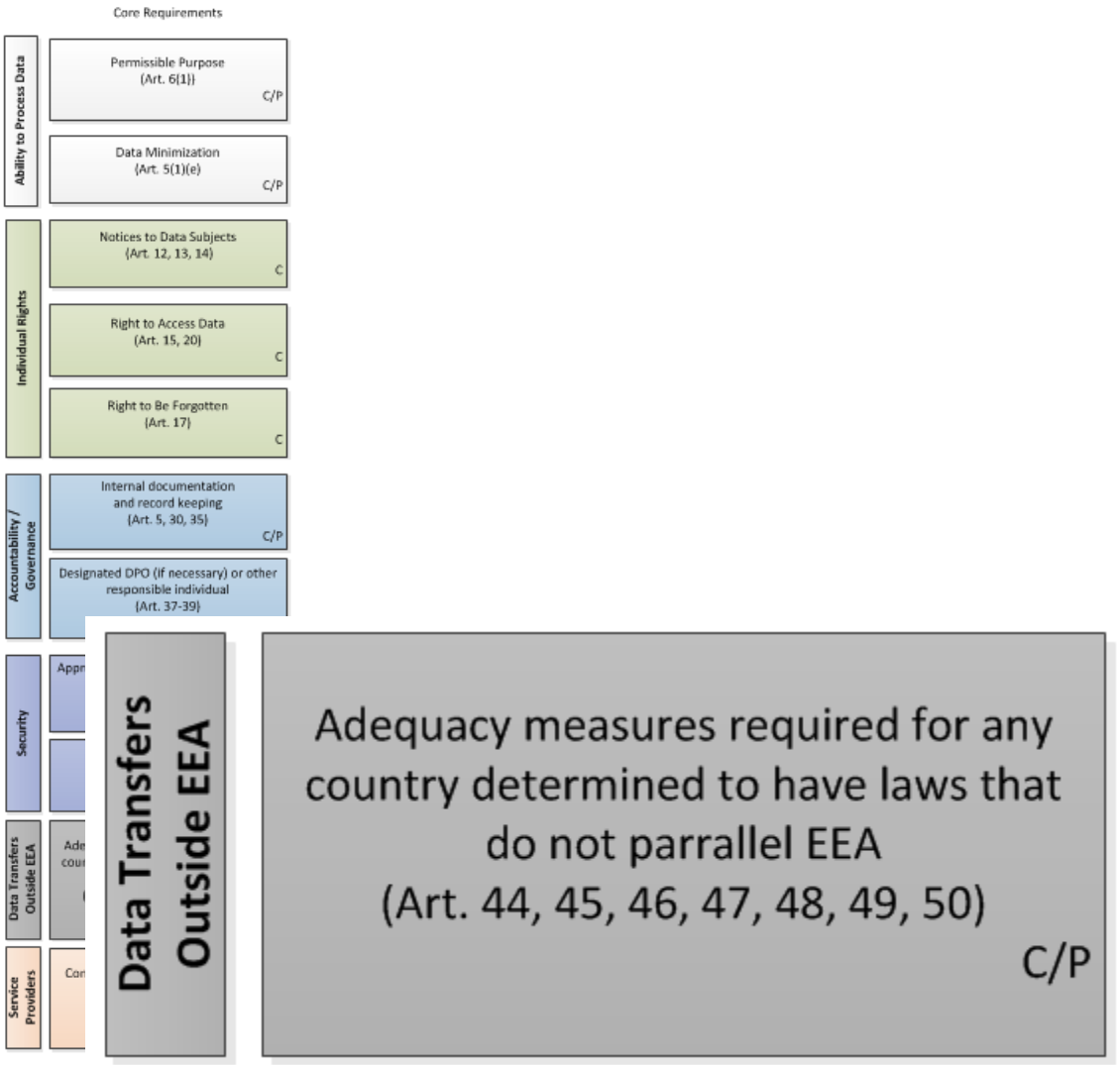


Overview: Data Security



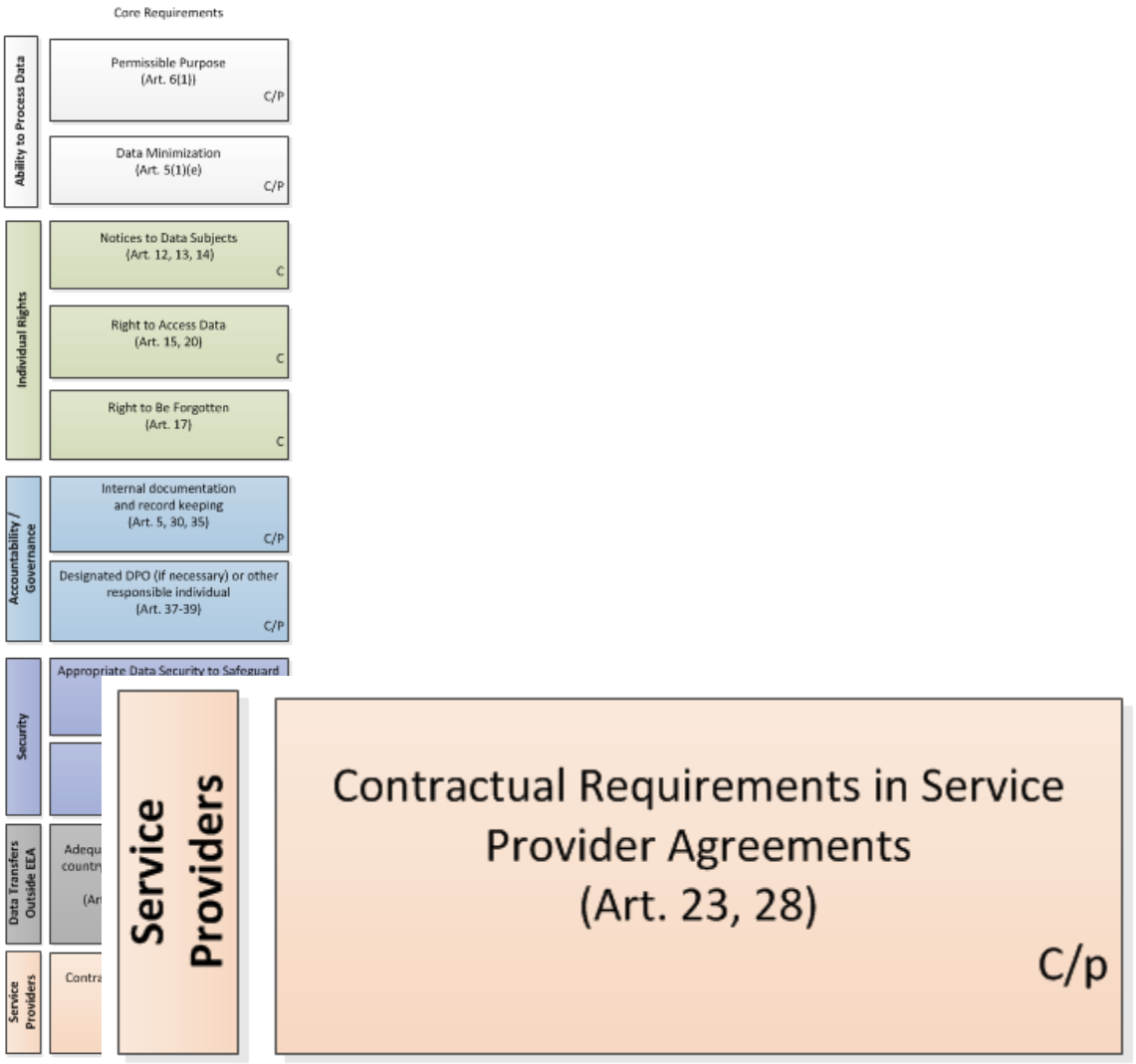
BRYAN CAVE

Overview: Transferring Data Outside EEA



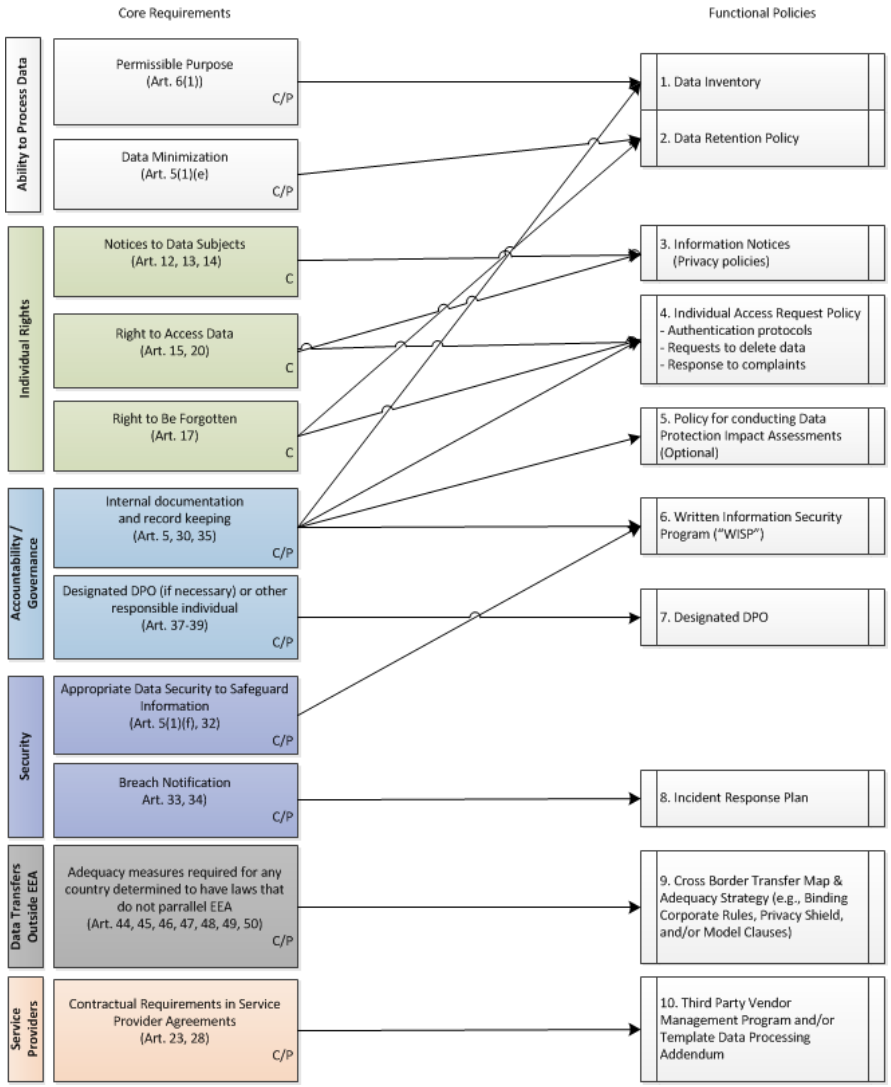
BRYAN CAVE

Overview: Service Providers



BRYAN CAVE

Overview: Operationalizing the GDPR – Top 10 Core Documents



BRYAN CAVE

Module 1: Conducting Data Inventories

Outline:

- What is a data inventory?
- Why do data inventories help with GDPR Compliance?
- Examples of data inventories
- Practice Pointers

Module 1: What is a data inventory?

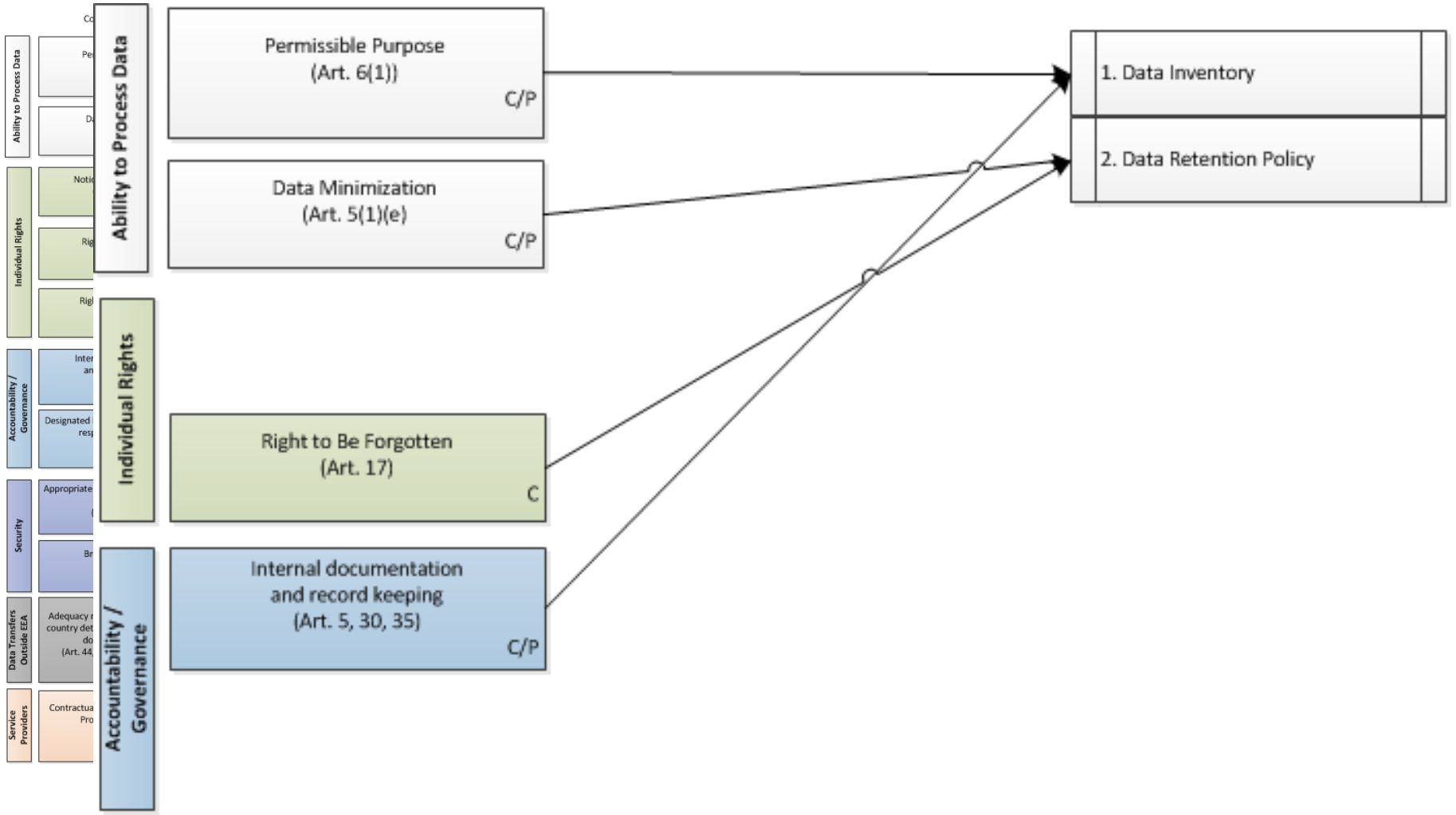
Data Inventory [noun]

> "Also known as a record of authority, identifies personal data as it moves across various systems and thus how data is shared and organized, and its location. That data is then categorized by subject area, which identifies inconsistent data versions, enabling identification and mitigation of data disparities."
>
> -International Association of Privacy Professional ("IAPP") Glossary of Privacy Terms

Synonyms:

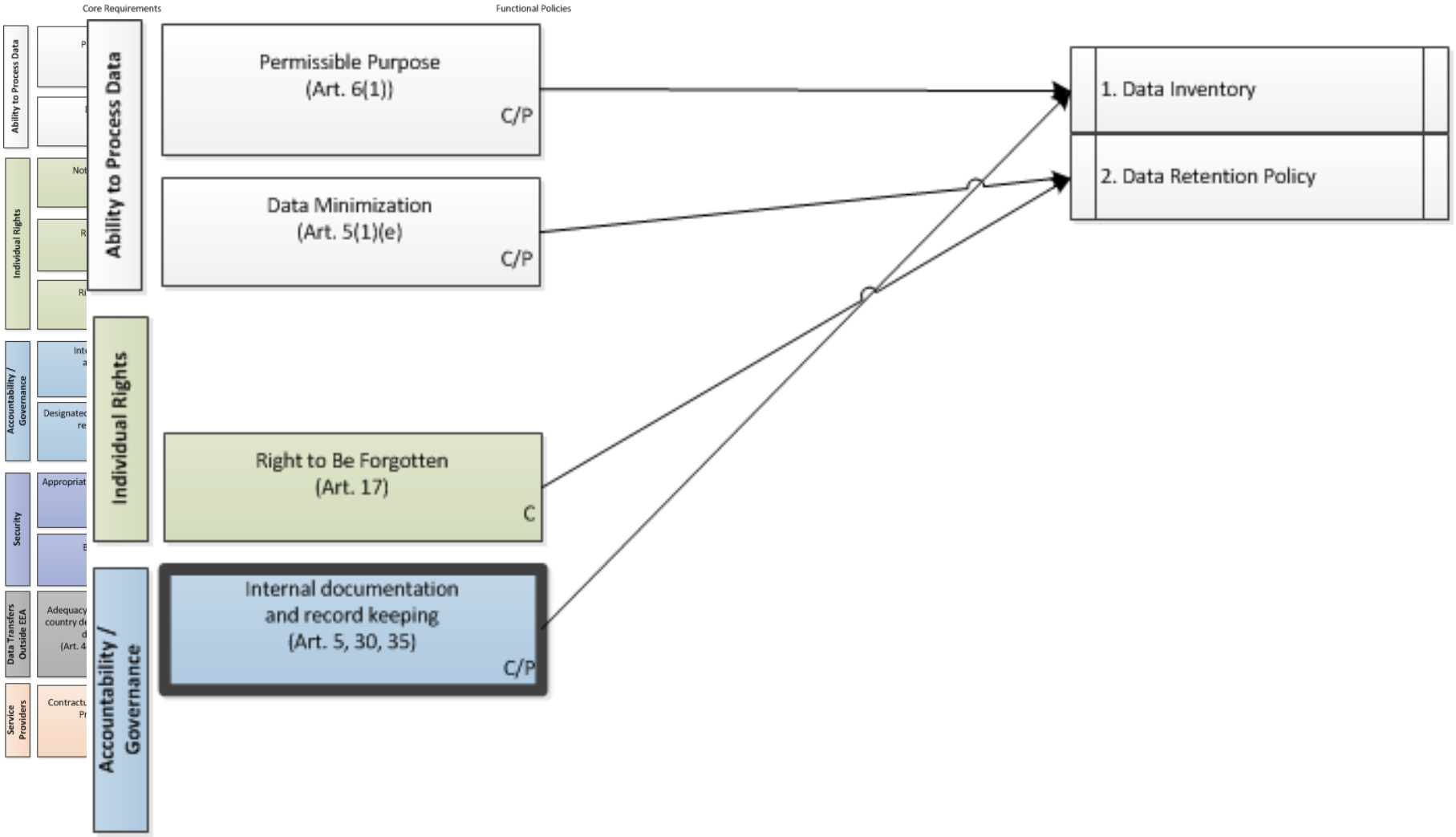
- Data map
- Data flow diagram
- Data register

Module 1: Why do data inventories help with GDPR Compliance?



BRYAN CAVE

Module 1: Article 30



Module 1: Article 30

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**:

. . .

(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 appropriate 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 Article32(1).

Module 1: Article 30

Article 30
Records of processing activities

…

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) …
(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 appropriate safeguards;
(d) where possible, **a general description of the technical and organisational security measures** referred to in Article32(1).

Module 1: Article 30

Article 30
Records of processing activities

3. The **records referred to in paragraphs 1 and 2 shall be in writing**, including in electronic form.

4. The controller or the processor and, where applicable, the controller's or the processor's representative, **shall make the record available to the supervisory authority on request**.

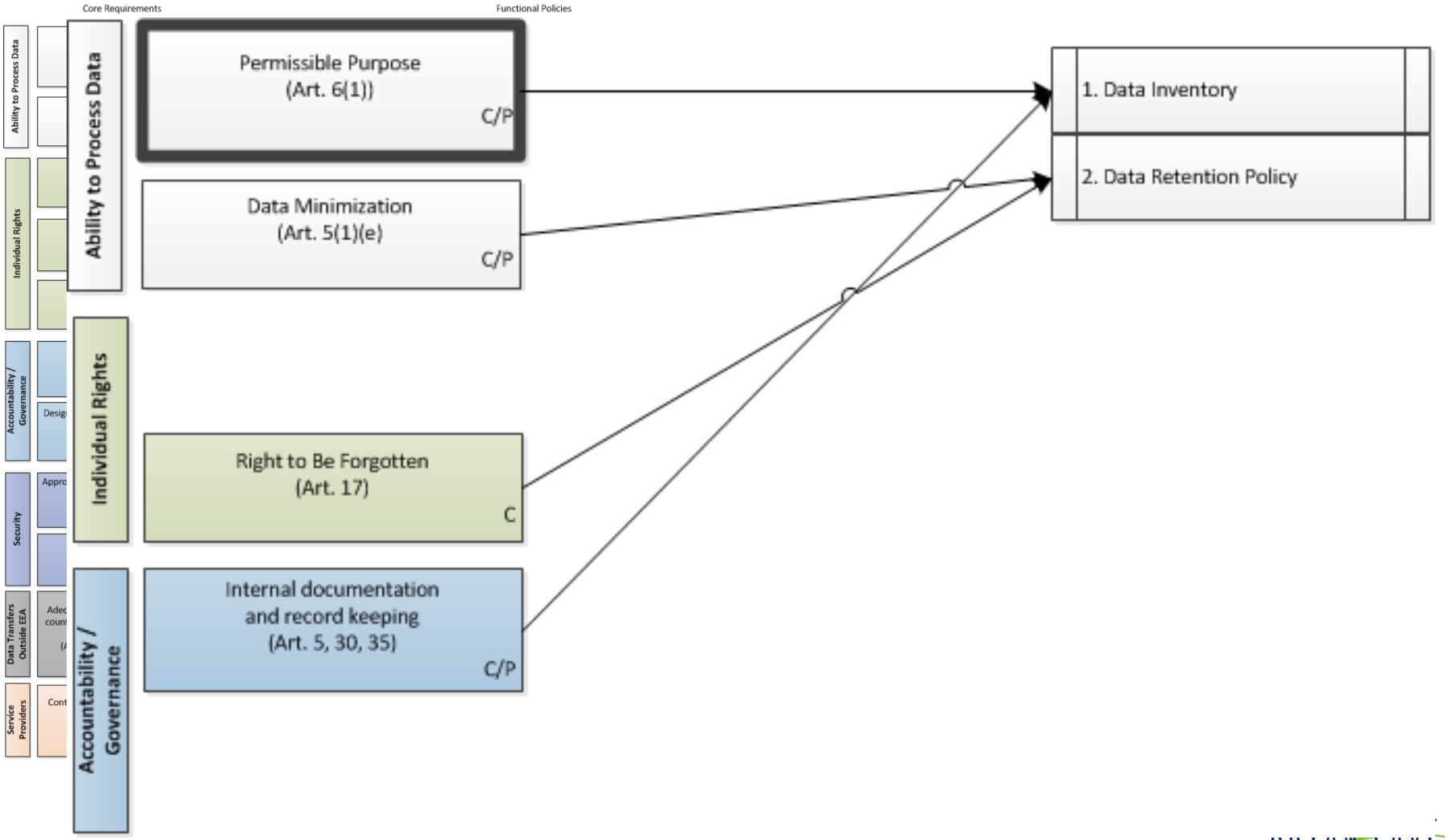
5. The **obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons** unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing 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.

Module 1: Article 30

Take-Aways from Article 30:

1. Most companies must keep a record of their processing.
2. (For Controllers) the record should describe:
   A. Purpose of processing
   B. Categories of data subjects
   C. Categories of personal data
   D. Categories of recipients of that data
   E. Cross-border transfers
   F. Time limits for erasure
   G. Security measures utilized

Module 1: Article 6(1)



Module 1: Article 6(1)

Article 6
Lawfulness of processing

1. Processing shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
(c) processing is necessary for compliance with a legal obligation to which the controller is subject;
(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

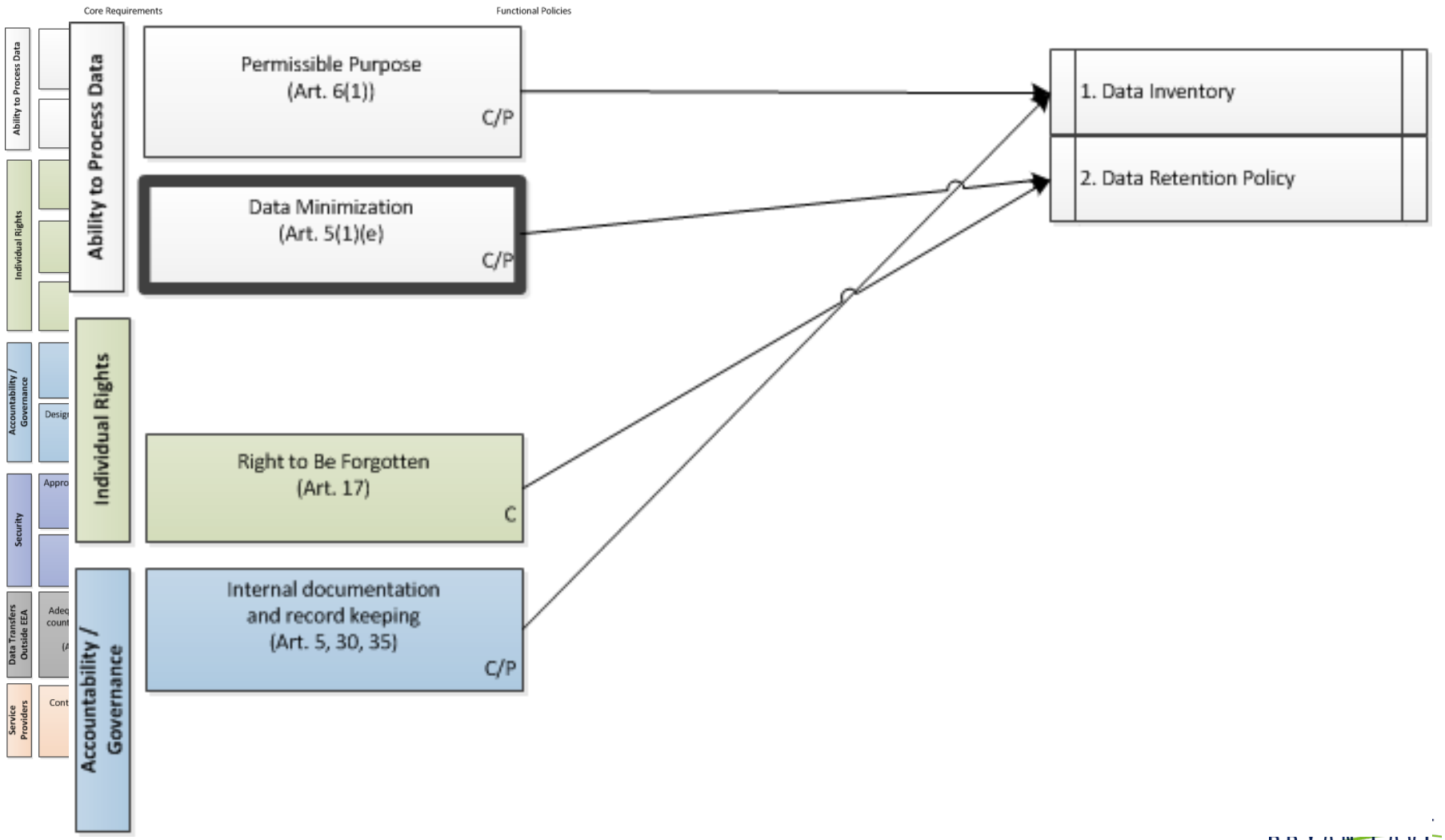
Module 1: Article 6(1)

Take-Aways from Article 6

You can only process data if you can point to one of the following reasons:

1. Data subject's consent.
2. Necessary to perform under a contract with the person.
3. Necessary to comply with a legal obligation;
4. Necessary to protect a person;
5. Necessary for the public interest;
6. Necessary for the controller's legitimate interests and those interests are not overridden by privacy concerns.

Module 1: Why do data inventories help with GDPR Compliance?



Module 1: Article 5(1)(e)

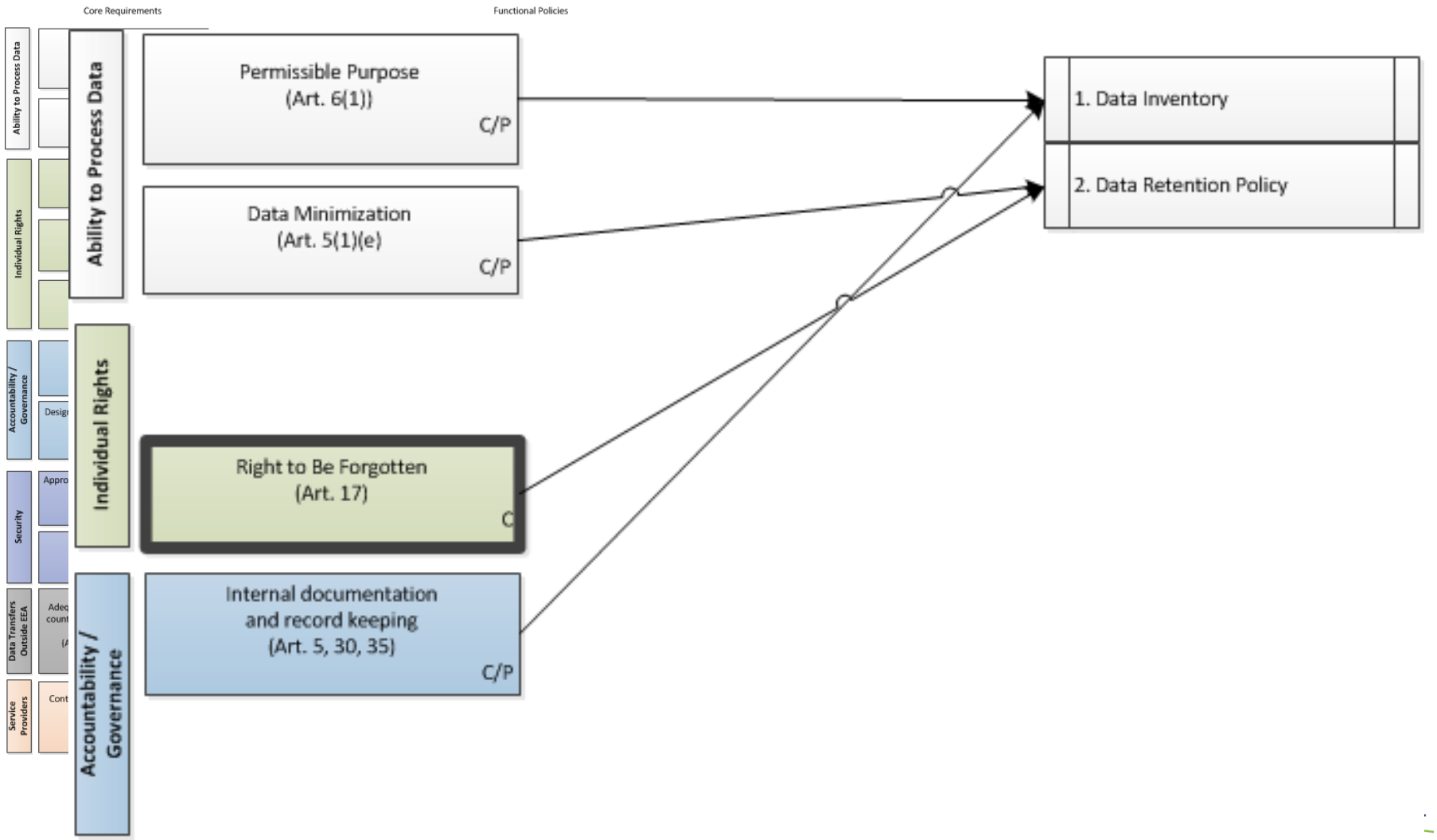
Article 5
Principles relating to processing of personal data

1. Personal data shall be:

…

(e) kept in a form which permits identification of data subjects **for no longer than is necessary for the purposes for which the personal data are processed;** personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

Module 1: Why do data inventories help with GDPR Compliance?



Module 1: Article 17

Article 17
Right to erasure ('right to be forgotten')

1. The **data subject shall have the right to obtain** from the controller the **erasure of personal data concerning him** or her without undue delay and the **controller shall have the obligation to erase personal data** without undue delay **where one of the following grounds applies**:

(a) the personal data are **no longer necessary in relation to the purposes** for which they were collected or otherwise processed;

(b) the **data subject withdraws consent on which the processing is based** according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;

(c) the **data subject objects to the processing pursuant to Article 21(1**) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article21(2);

(d) the personal data have been unlawfully processed;

(e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

(f) the personal data have been collected in relation to the offer of information society services referred to in Article8(1).

…

Module 1: Article 17

Take-Aways from Article 17

If someone requests that you delete information about them, whether you have to honor that requests depends on:

(1) Why you collected the information in the first place

(2) Whether that collection was based only on their consent.

(3) Whether that collection was based only on the controller's "legitimate interest."

Module 1: Examples of Data Inventories

- There is no one “right” way to conduct a data inventory.
- Companies take a variety of different approaches including:
  - Tasking someone to go out and conduct an inventory.
  - Retaining a consultant to go out and conduct an inventory.
  - Leveraging electronic survey tools.
  - Using Excel spreadsheets.
  - Creating elaborate graphical depictions of data
  - Utilizing electronic tools to search for personal data on networks.
  - Having system owners report information about systems as a policy.

Module 1: Examples of Data Inventories

- EU Data Protection Authorities have published some templates and examples.
  - *Commission Nationale de l'Informatique et des Libertés*

Identification of processing				Actors	Purpose of processing	Transfer outside EU?	Sensitive Data?
Name / logo	N° / REF	Date of creation	Last update	Responsible person for processing	Main purpose	Yes / No	Yes / No

BRYAN CAVE

Module 1: Examples of Data Inventories

- *German approach (multiple DPAs)*

Designation of the processing activity	Annex
Creation date:	Last modification date:
Responsible Department Contact Telephone Email address	
Designation of the processing activity	
Purposes of the processing	

BRYAN CAVE

Module 1: Examples of Data Inventories

- *German approach (multiple DPAs)*

Description of the categories of data subjects	❑ Employees ❑ Interested parties ❑ Suppliers ❑ Customers ❑ Patients ❑ Other:
Description of the categories of personal data	❑ ❑ ❑ Other: Special categories of personal data:

BRYAN CAVE

Module 1: Examples of Data Inventories

- *German approach (multiple DPAs)*

Categories of recipients to whom personal data have been or will be disclosed	❑ internal Department / Function
	❑ external Category of recipients
Transfer of personal data	❑ Transfer of personal data does not take place and is not planned ❑ Transfer of personal data takes place as follows: ❑ Third country, Name: ❑ International Organization, Designation:

BRYAN CAVE

Module 1: Examples of Data Inventories

- *German approach (multiple DPAs)*

Designation of the specific recipients of personal data	Category of recipients
In the case of a transfer referred to in Article 49(1), second subparagraph 2 GDPR.	Documentation of suitable safeguards
Time limits for erasure of the different categories of data	

Technical and organizational measures (TOM) referred to in Article 32(1) GDPR Comments:

BRYAN CAVE

Module 1: Examples of Data Inventories

- *UK Information Commissioner's Office (ICO) Approach*

Business function	Purpose of processing	Name and contact details of joint controller (if applicable)	Categories of individuals	Categories of personal data
Finance	Payroll	N/A	Employees	Contact details
Finance	Payroll	N/A	Employees	Bank details
Finance	Payroll	N/A	Employees	Pension details
Finance	Payroll	N/A	Employees	Tax details
Human Resources	Personel file	N/A	Employees	Contact details
Human Resources	Personel file	N/A	Employees	Pay details
Human Resources	Personel file	N/A	Employees	Annual leave details

Categories of recipients	Link to contract with processor	Names of third countries or international organsations that personal data are transferred to (if applicable)	Safeguards for exceptional transfers of personal data to third countries or international organisations (if applicable)	Retention schedule (if possible)
HMRC	N/A	N/A	N/A	5 years post-employment
HMRC	N/A	N/A	N/A	3 years post-employment
HMRC	N/A	N/A	N/A	75 years post-employment
HMRC	N/A	N/A	N/A	6 years post-employment
N/A	N/A	N/A	N/A	6 years post-employment
N/A	N/A	N/A	N/A	6 years post-employment
N/A	N/A	N/A	N/A	6 years post-employment

Module 1: Examples of Data Inventories

- *UK Information Commissioner's Office (ICO) Approach*

General description of technical and organisational security measures (if possible)	Article 6 lawful basis for processing personal data	Article 9 basis for processing special category data	Legitimate interests for the processing (if applicable)	Link to record of legitimate interests assessment (if applicable)
Encrypted storage and transfer	Article 6(1)(c) - legal obligation	N/A	N/A	N/A
Encrypted storage and transfer	Article 6(1)(c) - legal obligation	N/A	N/A	N/A
Encrypted storage and transfer	Article 6(1)(c) - legal obligation	N/A	N/A	N/A
Encrypted storage and transfer	Article 6(1)(c) - legal obligation	N/A	N/A	N/A
Encrypted storage	Article 6(1)(b) - contract	N/A	N/A	N/A
Encrypted storage, access controls	Article 6(1)(b) - contract	N/A	N/A	N/A
Encrypted storage, access controls	Article 6(1)(b) - contract	N/A	N/A	N/A

Rights available to individuals	Existence of automated decision-making, including profiling (if applicable)	The source of the personl data (if applicable)	Link to record of consent	Location of personal data
Access and rectification	No	Data subject	N/A	Finance payroll system
Access and rectification	No	Data subject	N/A	Finance payroll system
Access and rectification	No	Controller	N/A	Finance pension system
Access and rectification	No	Controller	N/A	Finance payroll system
Access, data portability, rectification	No	Data subject	N/A	HR personel system
Access, data portability, rectification	No	Controller	N/A	HR personel system
Access, data portability, rectification	No	Data subject	N/A	HR personel system

Module 1: Examples of Data Inventories

- *UK Information Commissioner's Office (ICO) Approach*

Data Protection Impact Assessments			Personal Data Breaches	
Data Protection Impact Assessment required?	Data Protection Impact Assessment progress	Link to Data Protection Impact Assessment	Has a personal data breach occurred?	Link to record of personal data breach
No	N/A	N/A	No	N/A
No	N/A	N/A	No	N/A
No	N/A	N/A	No	N/A
No	N/A	N/A	No	N/A
No	N/A	N/A	No	N/A
No	N/A	N/A	No	N/A
No	N/A	N/A	No	N/A

Data Protection Bill - Special Category or Criminal Conviction and Offence data				
Data Protection Bill Schedule Condition for processing	GDPR Article 6 lawful basis for processing	Link to retention and erasure policy document	Is personal data retained and erased in accordance with the policy document?	Reasons for not adhering to policy document (if applicable)
N/A	N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A	N/A

Module 1: Practice Pointers

1. Data inventories are a process; not an event.
2. Whatever system you put into place has to be replicable.
3. Low-tech solutions can be attractive but can lead to unexpected complexities particularly around organization and coordination with system owners.
4. High-tech solutions can be costly and may not be replicable.
5. Striking the balance between information that is too high level to be useful or information that is so granular it can never be collected is difficult.

Module 1: Biography

David Zetoony
Partner
Chair, Data Privacy & Security Team

Bryan Cave LLP
Washington, D.C. / Boulder, Colorado
202 508 6030
David.Zetoony@bryancave.com

David Zetoony is the leader of the firm's global data privacy and security practice. He has extensive experience advising clients on how to comply with state and federal privacy, security, and advertising laws, representing clients before the Federal Trade Commission, and defending national class actions. He has assisted hundreds of companies in responding to data security incidents and breaches, and has represented human resource management companies, financial institutions, facial recognition companies, and consumer tracking companies before the Federal Trade Commission on issues involving data security and data privacy.

BRYAN CAVE

bryancave.com | A Global Law Firm