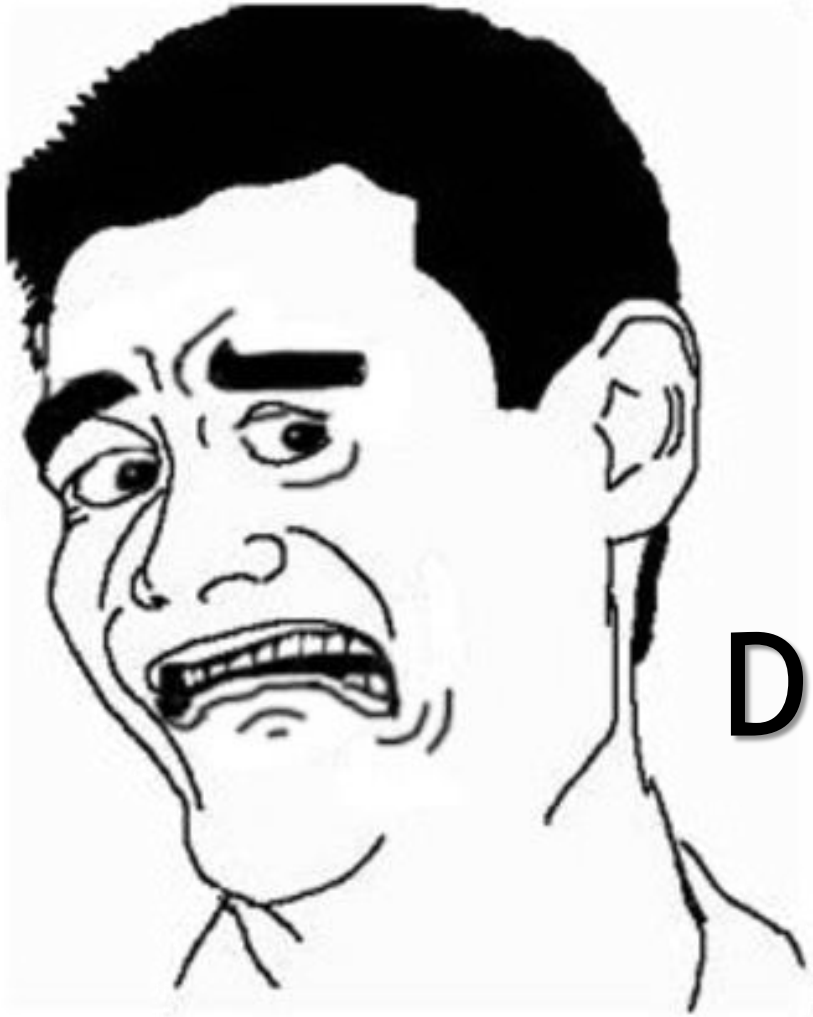
GDPR & Fundamentals of IG

RICOH USA



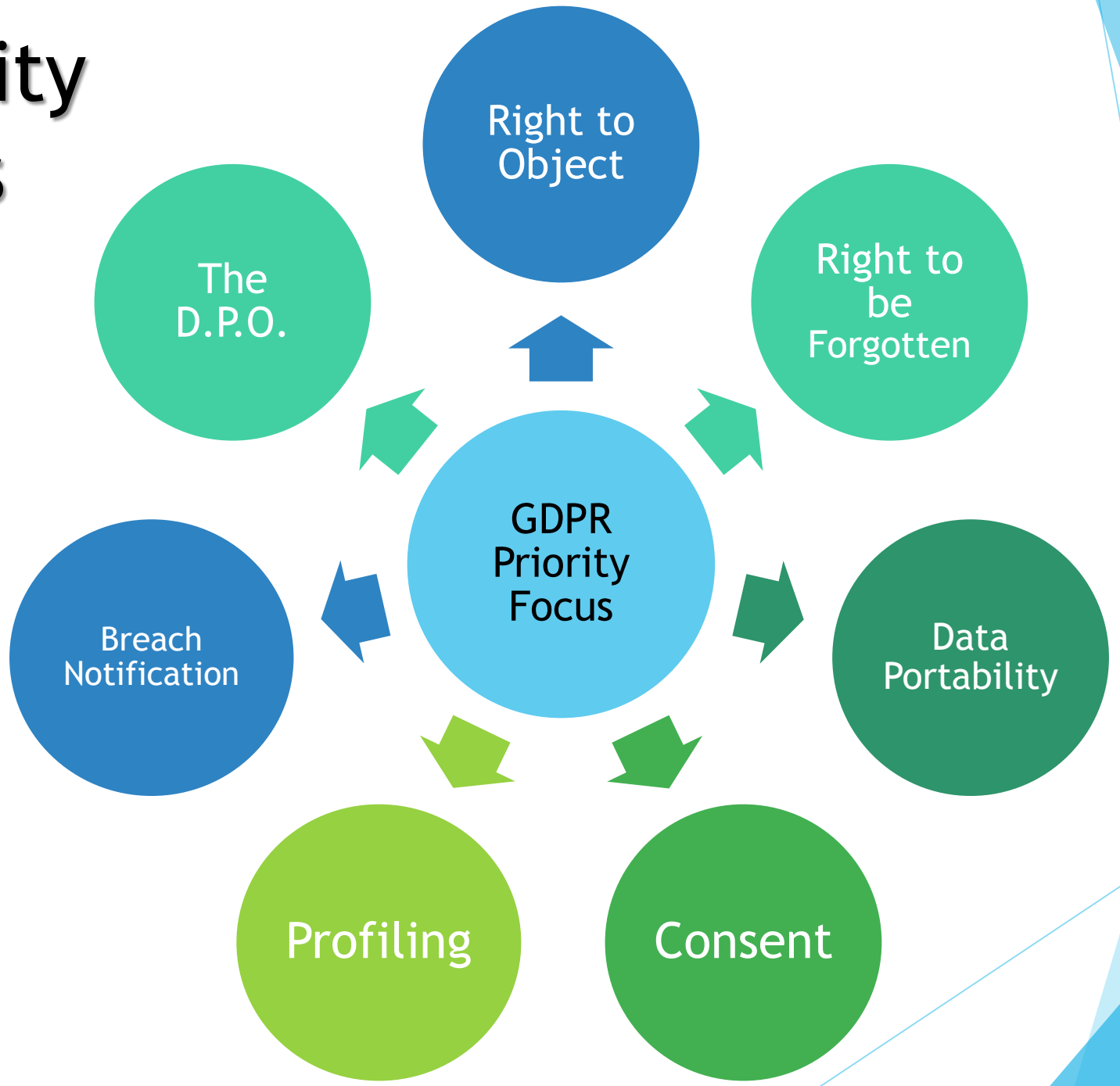
Darn **GDPR. Again?**

We have been all over the place when it comes to GDPR

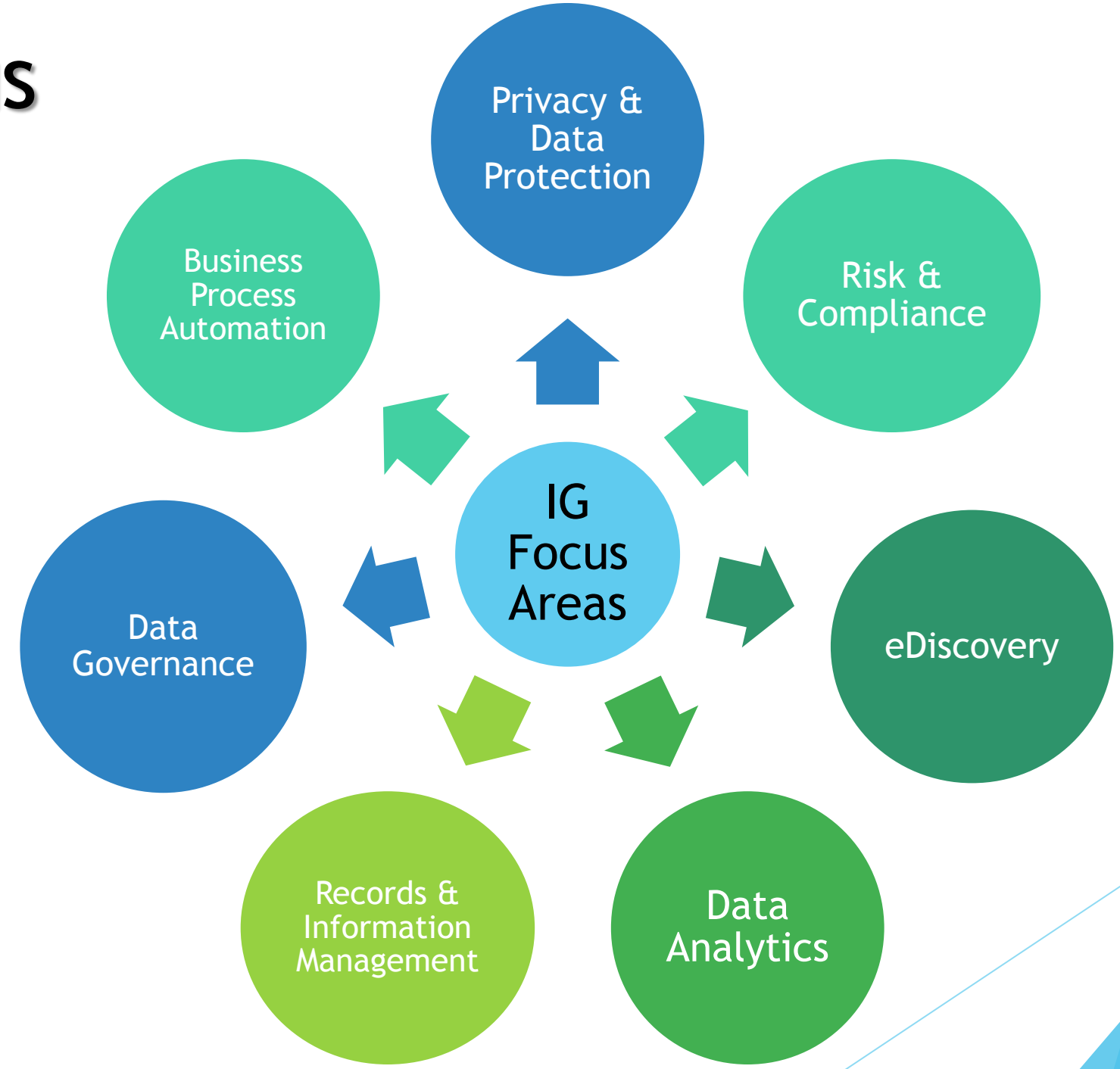
So what are the main concerns for organizations?

So what does Information Governance address for organizations?

GDPR Priority focus areas



IG Focus Areas



IG Focus Areas mapped to IG Initiatives/Projects

- ✓ Information Governance Committee
- ✓ Policies and Procedures
- ✓ Records Retention Schedule
- ✓ Enterprise Content Management System
- ✓ Records Management System (Physical and Electronic)
- ✓ Content Analytics
- ✓ File Classification
- ✓ Taxonomy
- ✓ Information Map (Structured and Unstructured)
- ✓ Data Governance
- ✓ Information Security
- ✓ E-Discovery
- ✓ Legal Hold Notification System
- ✓ Organizational Change Management

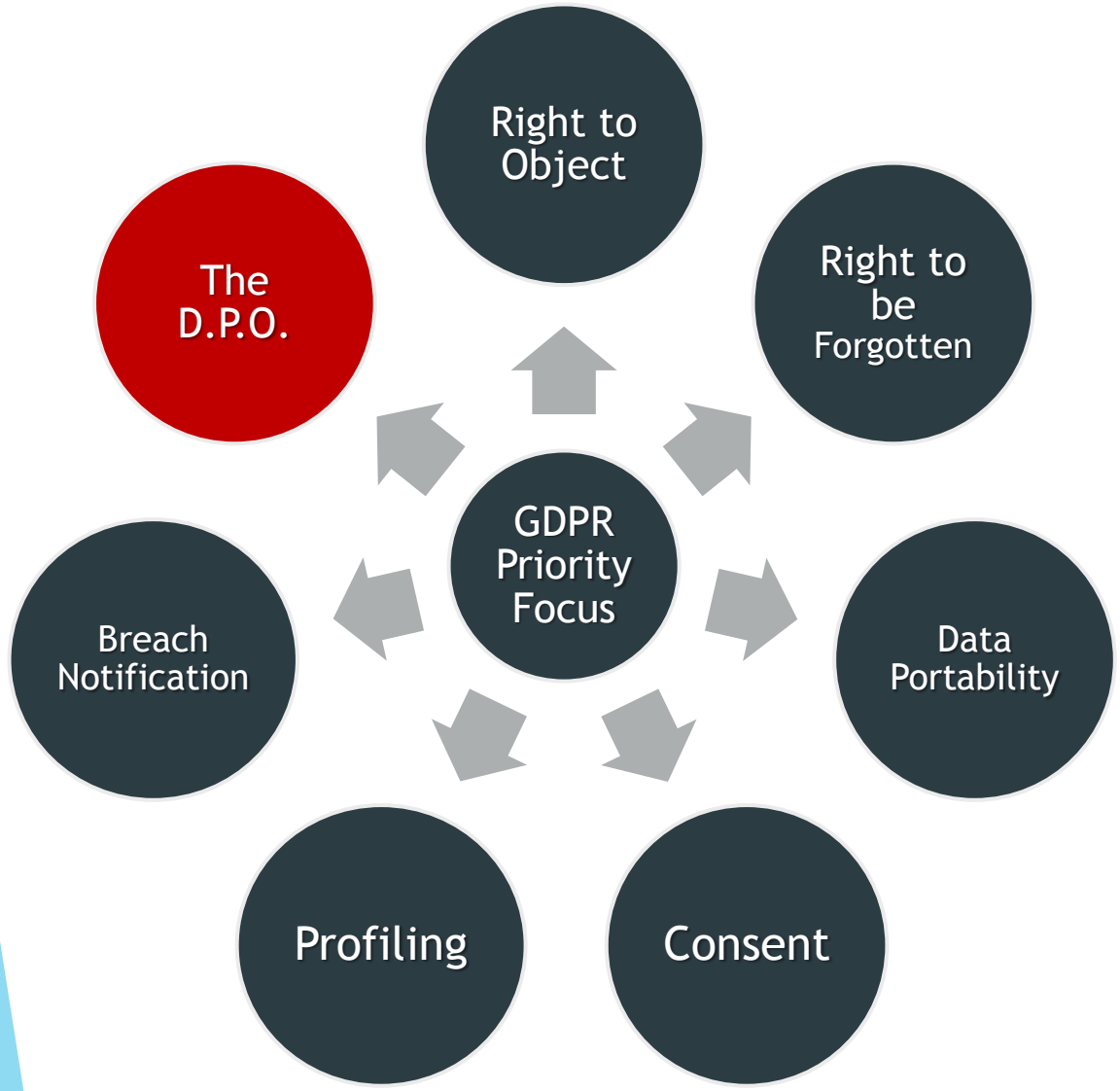
Article 37, 38, 39 GDPR: The D.P.O.

- The Controller or Processor Shall designate a D.P.O where
  - Processing is carried out by a public authority or body
  - Their core activities require regular and systematic monitoring of data subjects
  - Their core activities consist of processing large quantities of special categories of data

- There maybe a single D.P.O. for a group of companies keeping accessibility in mind
  - A single D.P.O. maybe appointed for several public authorities or bodies

- The D.P.O should be
  - Expert in the knowledge of data protection law and practices
  - Directly reporting to the highest management level
  - Bound by secrecy and confidentiality concerning the performance of his or her tasks

- Reference Articles under GDPR
  - Article 37 – Designation of a Data Protection Officer
  - Article 38 – Position of the Data Protection Officer
  - Article 39 – Tasks of the Data Protection Officer



- ✓ **Information Governance Committee**
- ✓ **Policies and Procedures**
- ✓ Records Retention Schedule
- ✓ Enterprise Content Management System
- ✓ Records Management System (Physical and Electronic)
- ✓ Content Analytics
- ✓ File Classification
- ✓ Taxonomy
- ✓ Information Map (Structured and Unstructured)
- ✓ Data Governance
- ✓ **Information Security**
- ✓ E-Discovery
- ✓ Legal Hold Notification System
- ✓ **Organizational Change Management**

Article 7 GDPR: Conditions for Consent

- Where the processing was based on consent the **controller must be able to demonstrate the data subjects consent to processing of personal data**.

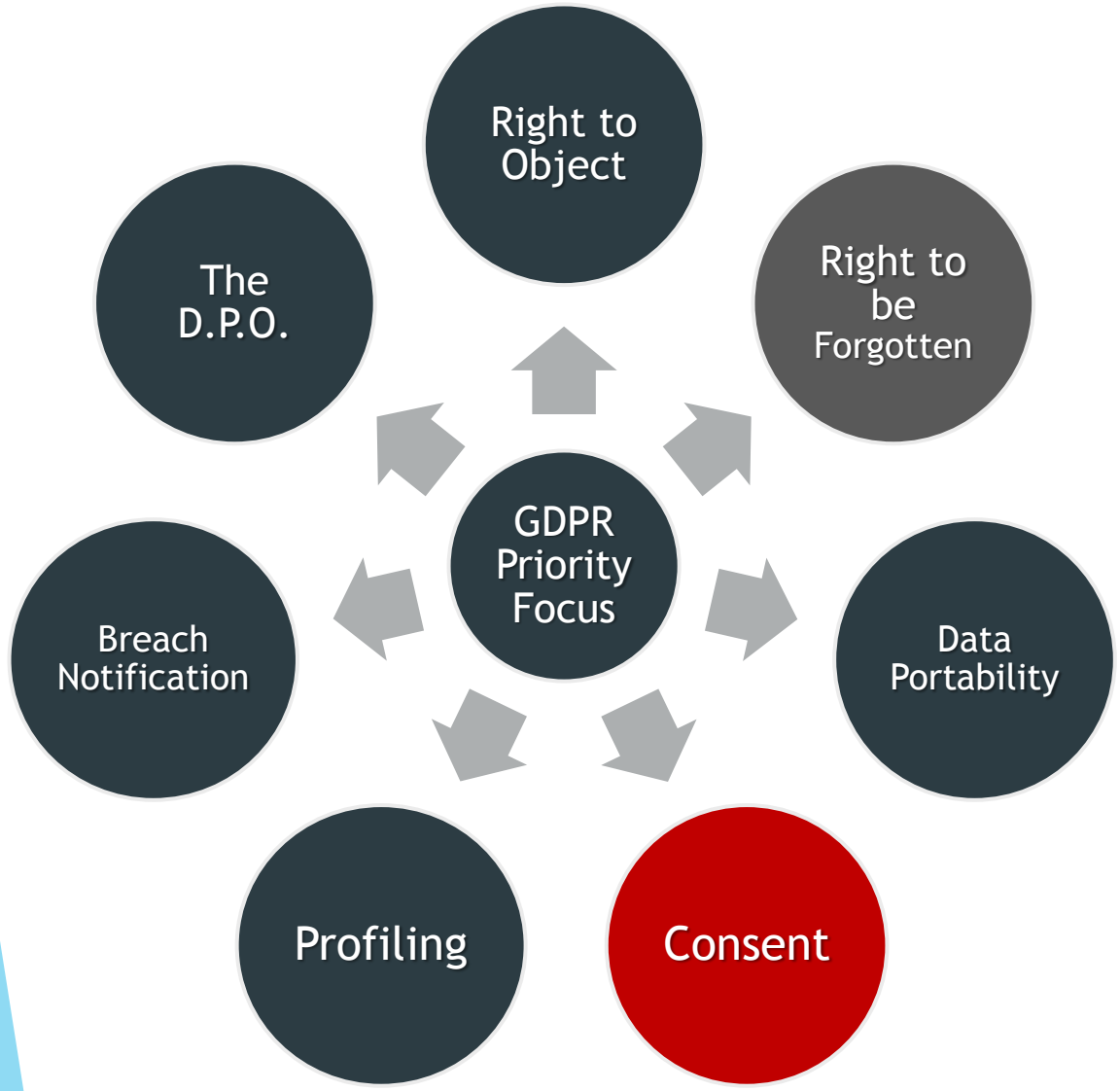
- Where consent is attained through a written declaration that concerns other matters the consent request must be:
  - Clearly distinguishable from other matters,
  - in an intelligible and easily accessible form, and
  - use clear and plain language

- **"Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding."**

- **Data subject has the right to withdraw consent at any time.**

- Prior to giving consent the data subject must be notified that **"it shall be as easy to withdraw as to give consent."**

- When determining whether consent is freely given, a primary consideration will be whether **performance of a contract is conditioned on the consent** to processing personal **data that is not necessary for performance** of that contract.



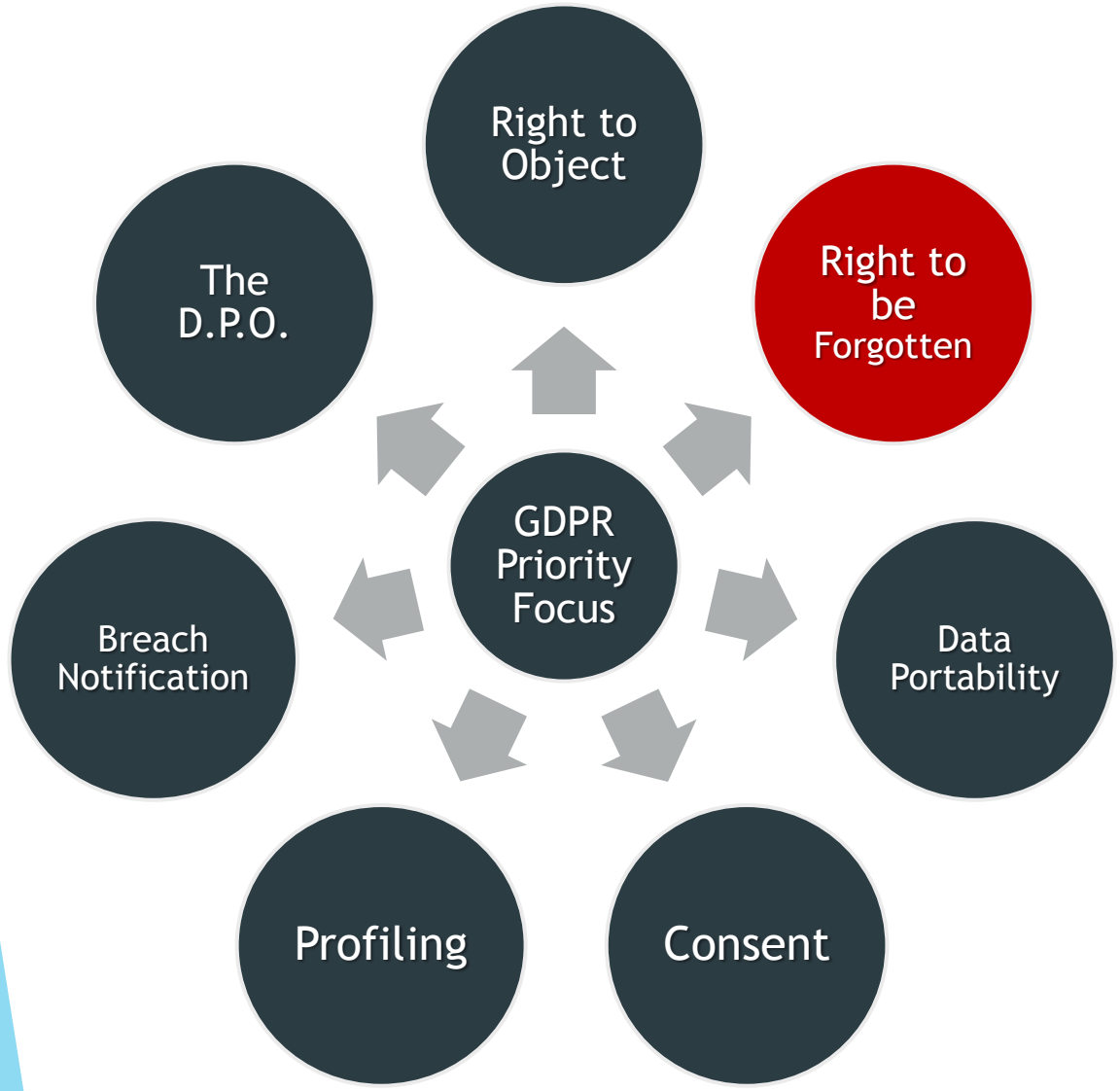
- ✓ **Information Governance Committee**
- ✓ **Policies and Procedures**
- ✓ Records Retention Schedule
- ✓ Enterprise Content Management System
- ✓ Records Management System (Physical and Electronic)
- ✓ Content Analytics
- ✓ File Classification
- ✓ Taxonomy
- ✓ Information Map (Structured and Unstructured)
- ✓ Data Governance
- ✓ Information Security
- ✓ **E-Discovery**
- ✓ Legal Hold Notification System
- ✓ **Organizational Change Management**

Article 17 GDPR: Right to be Forgotten

- Data subject has the right to erasure of personal data concerning him or her without undue delay
- The controller shall have the obligation to delete personal data when:
  - It is no longer necessary in relation to the purposes
  - The data subject withdraws consent
  - The data subject objects to the processing based on certain criteria
  - It has been unlawfully processed
  - There is a legal obligation based on the law

- When the controller has made the personal data public, they shall have to take reasonable steps, including technical measures, to inform other controllers regarding the data subjects' request of erasure

- The above will not apply
  - For reasons of public interest, scientific or historical research purposes or statistical purposes
  - For the establishment, exercise or defense of legal claims



- ✓ Information Governance Committee
- ✓ Policies and Procedures
- ✓ Records Retention Schedule
- ✓ Enterprise Content Management System
- ✓ Records Management System (Physical and Electronic)
- ✓ Content Analytics
- ✓ File Classification
- ✓ Taxonomy
- ✓ Information Map (Structured and Unstructured)
- ✓ Data Governance
- ✓ Information Security
- ✓ E-Discovery
- ✓ Legal Hold Notification System
- ✓ Organizational Change Management

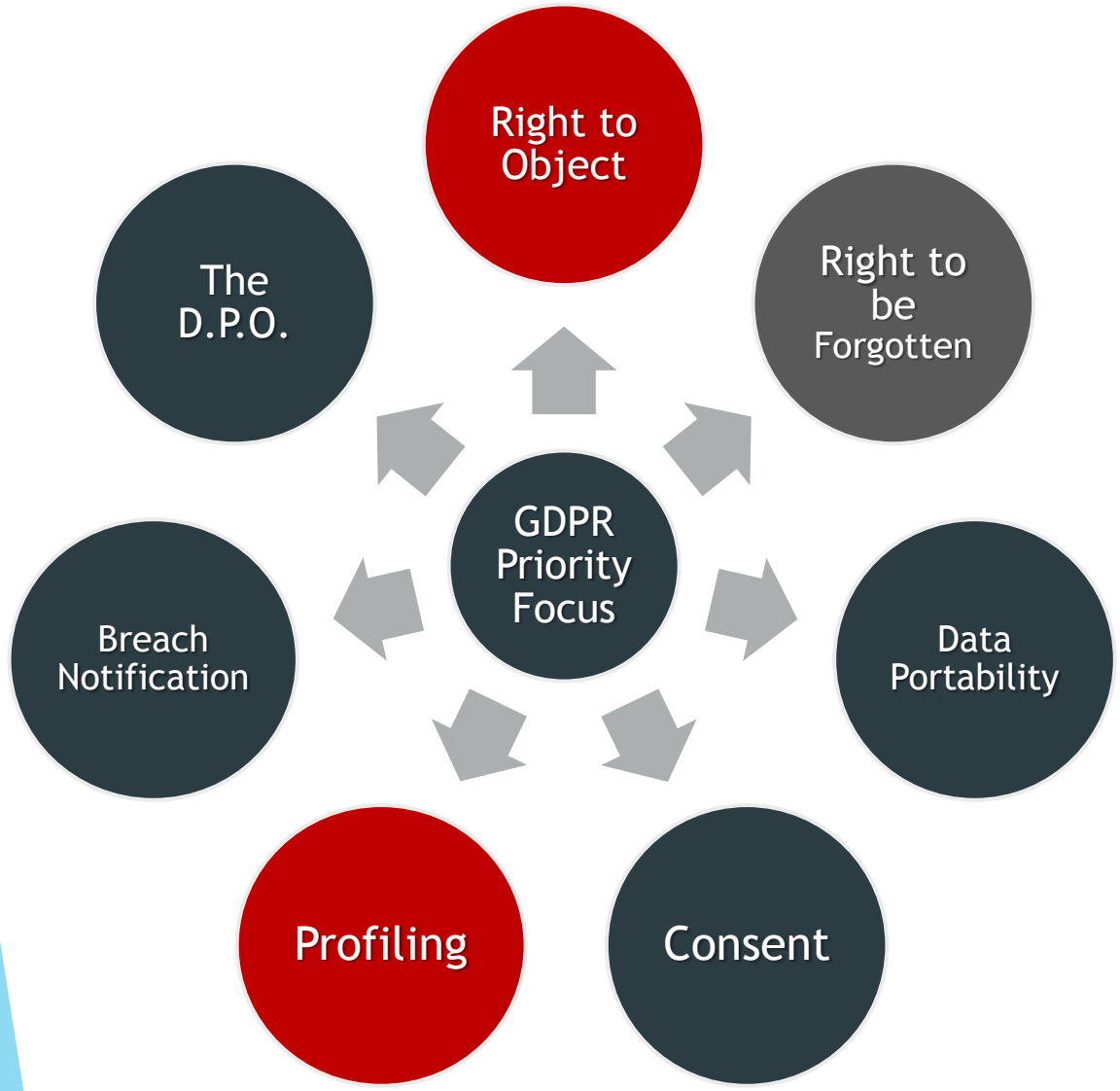
Article 21, 22 GDPR: Right to Object & Profiling

- The data subject has the rights to object
  - Where there are personal data processing concerns, including profiling
  - Where the data is being processed for direct marketing purpose

- The right to object shall be communicated to the data subject at the time of the first communication
  - It shall be presented clearly and separately from any other information

- The data subject may send in their objection by automated means using technical specifications

- The data subject may object to personal data being processed for scientific, historical or statistical purposes unless processing is necessary for reasons of public interest



- ✓ **Information Governance Committee**
- ✓ **Policies and Procedures**
- ✓ **Records Retention Schedule**
- ✓ **Enterprise Content Management System**
- ✓ **Records Management System (Physical and Electronic)**
- ✓ Content Analytics
- ✓ File Classification
- ✓ Taxonomy
- ✓ Information Map (Structured and Unstructured)
- ✓ Data Governance
- ✓ Information Security
- ✓ **E-Discovery**
- ✓ Legal Hold Notification System
- ✓ **Organizational Change Management**

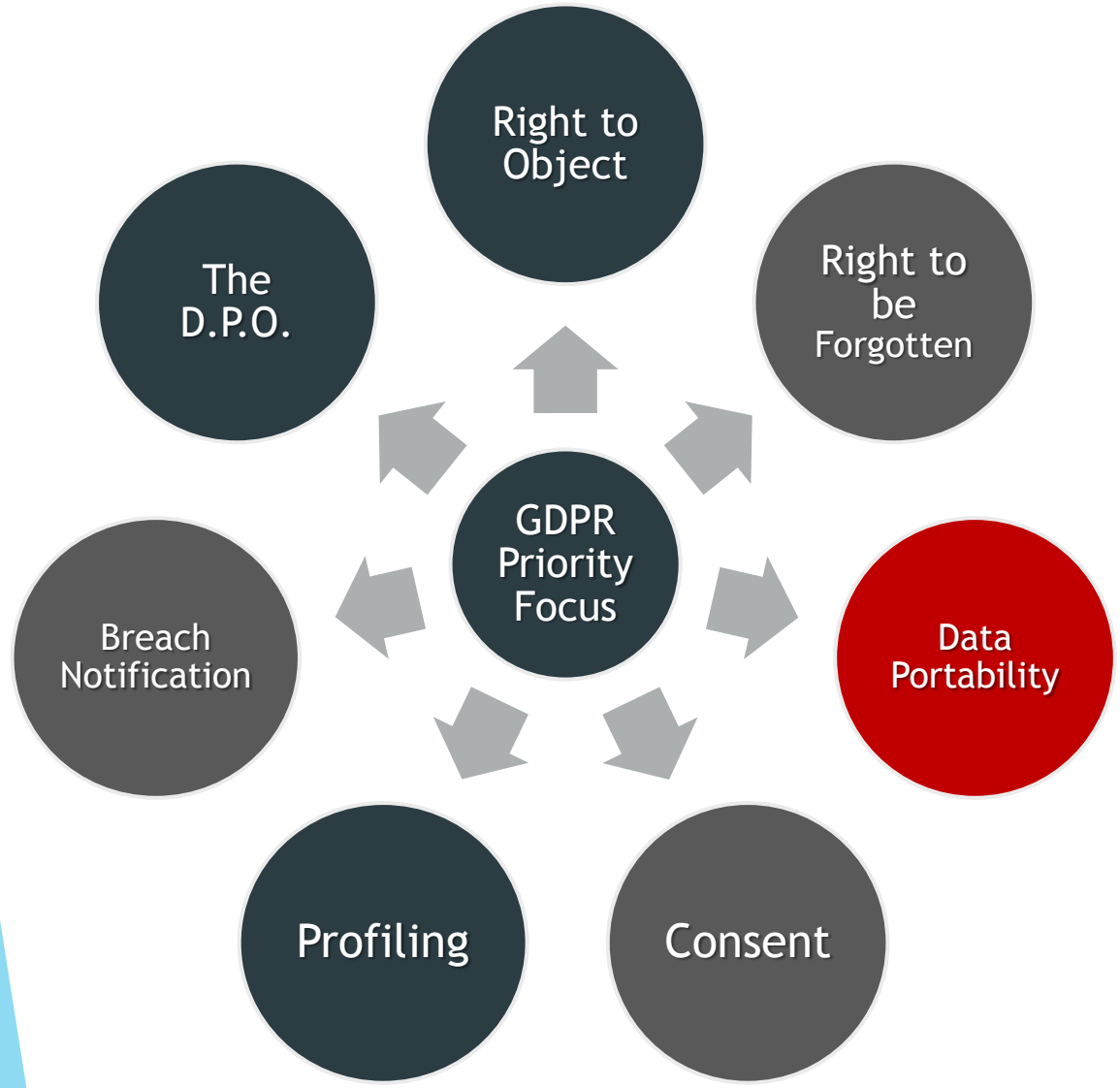
Article 20 GDPR: Right to Data Portability

- The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, **commonly used and machine-readable format** and have **the right to transmit those data to another controller** without hindrance from the controller to which the personal data have been provided, where:
    - consent is based on article 6.1.a, or
    - necessary for performance of a contract per article 6.1.b
  - and
    - processing is automated

- Right to have personal data **transmitted directly from one controller to another**, where technically feasible.

- Not applicable to processing necessary for performance of tasks in the
    - **public interest**, or
    - **exercise of official authority** vested in the controller

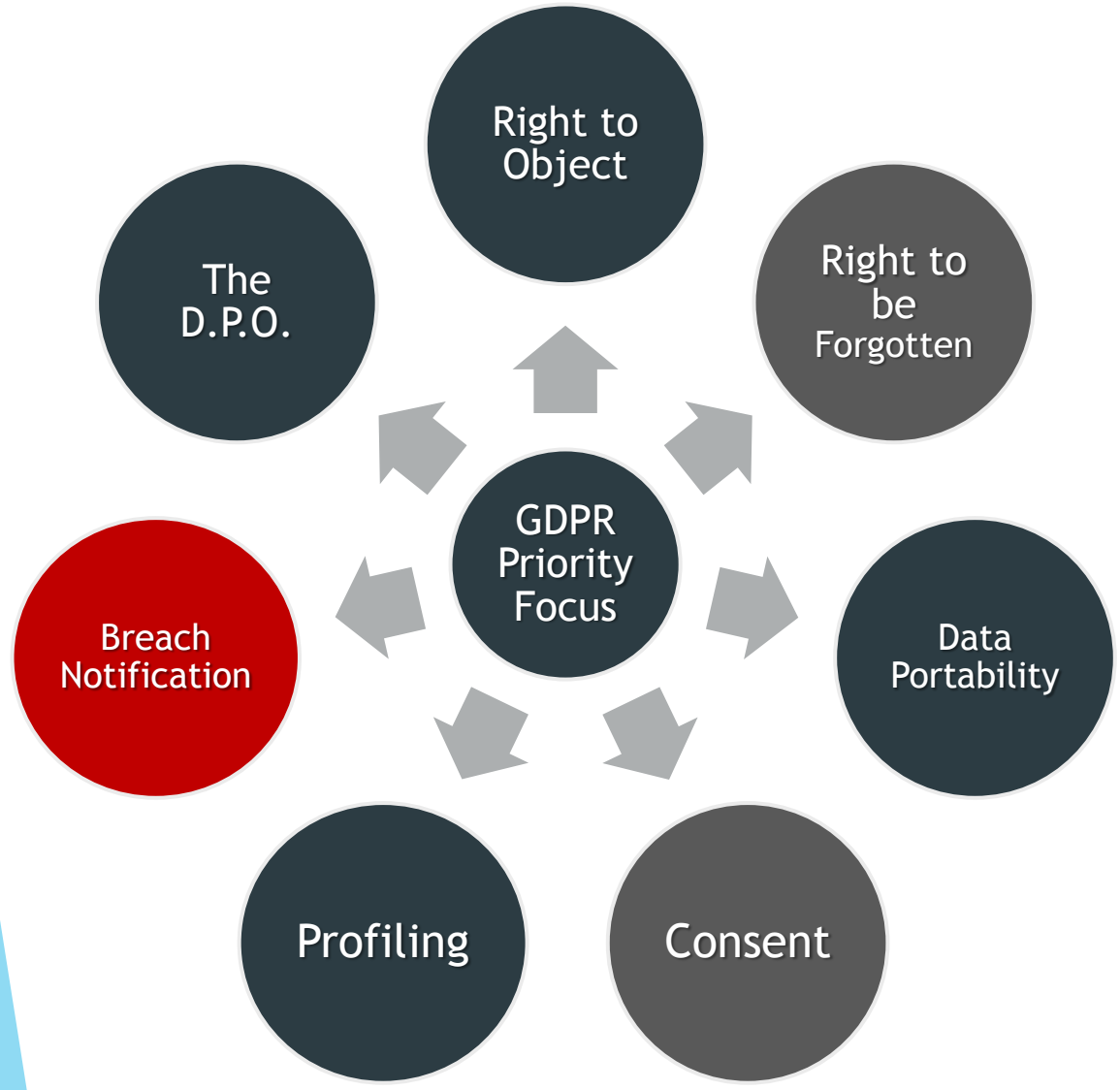
- Right to data portability must not adversely affect the rights and freedoms of others



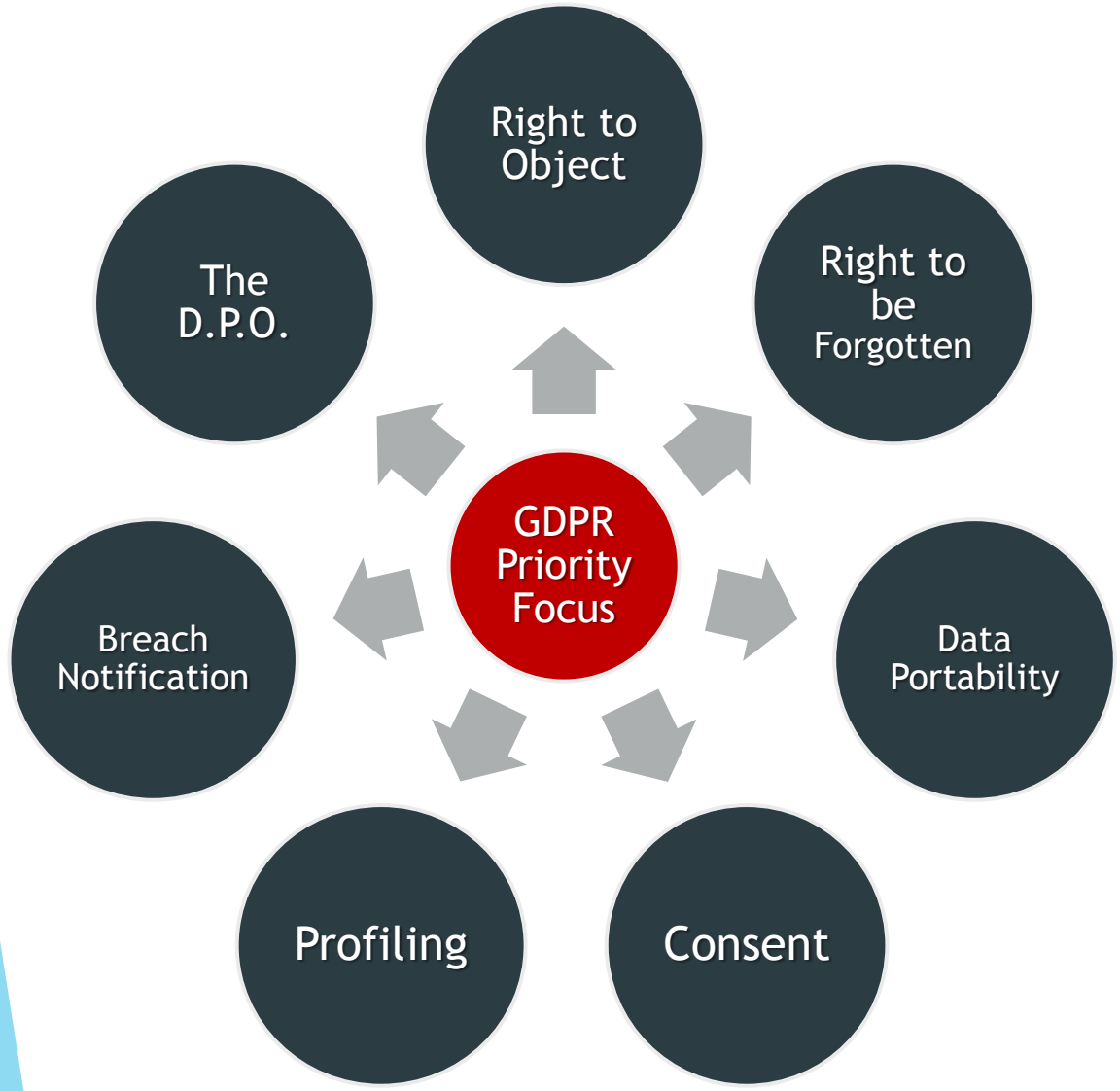
- ✓ **Information Governance Committee**
- ✓ **Policies and Procedures**
- ✓ Records Retention Schedule
- ✓ Enterprise Content Management System
- ✓ Records Management System (Physical and Electronic)
- ✓ Content Analytics
- ✓ File Classification
- ✓ Taxonomy
- ✓ **Information Map (Structured and Unstructured)**
- ✓ **Data Governance**
- ✓ **Information Security**
- ✓ **E-Discovery**
- ✓ **Legal Hold Notification System**
- ✓ **Organizational Change Management**

Article 33 GDPR: Breach Notification

- Processor shall notify the controller **without undue delay** after becoming aware of a personal data breach
- Once aware that a data breach has occurred the controller shall notify the competent supervisory authority
  - without undue delay, and
  - where feasible, not later than 72 hours(If later than 72 hours notification must include reasoning for delay)
- **Notifying the supervisory authority is not required where the breach is unlikely to result in a risk to the rights and freedoms of natural persons.**
- Notification shall include **at least**:
  - the nature of the breach including, where possible
    - categories and approximate number of data subjects, and
    - categories and approximate number of data records
  - the name and contact information of the DPO, or other point of contact
  - the likely consequences of the breach
  - the measures taken or proposed to be taken by the controller to address the breach including, where appropriate measures to mitigate possible adverse effects
- Information may be provided in phases without further undue delay where providing it at one time is not possible
- The controller is required to document any personal data breaches including
  - facts surrounding the breach
  - the effects of the breach
  - actions taken to remediate the breach
- The documentation shall enable the supervisory authority to verify compliance with Article 33 requirements



- ✓ **Information Governance Committee**
- ✓ **Policies and Procedures**
- ✓ Records Retention Schedule
- ✓ Enterprise Content Management System
- ✓ Records Management System (Physical and Electronic)
- ✓ **Content Analytics**
- ✓ **File Classification**
- ✓ Taxonomy
- ✓ **Information Map (Structured and Unstructured)**
- ✓ **Data Governance**
- ✓ **Information Security**
- ✓ **E-Discovery**
- ✓ **Legal Hold Notification System**
- ✓ **Organizational Change Management**



- ✓ Information Governance Committee
- ✓ Policies and Procedures
- ✓ Records Retention Schedule
- ✓ Enterprise Content Management System
- ✓ Records Management System (Physical and Electronic)
- ✓ Content Analytics
- ✓ File Classification
- ✓ Taxonomy
- ✓ Information Map (Structured and Unstructured)
- ✓ Data Governance
- ✓ Information Security
- ✓ E-Discovery
- ✓ Legal Hold Notification System
- ✓ Organizational Change Management

Q & A

Jonathan Schieber, Esq., IGP

Principal Consultant – Governance, Risk & Compliance

Ricoh USA

- Over 10+ years experience as eDiscovery Counsel at a top 5 nationwide law firm
- Intimate understanding of the pitfalls, risks & costs associated with weak governance.
- Develops strategies, workflows & Systems to empower clients to proactively manage their data.

Kedar Thakkar, CIP, IGP

Principal Consultant – Governance, Risk & Compliance

Ricoh USA

- 20+ years of experience in various roles including RIM practitioner, IG Consulting and IT administration & architecture
- Develops robust IG programs where information assets are identified, protected and leveraged for value.
- Experienced in addressing IG concerns throughout corporate acquisitions, facility closures and technology transformations.