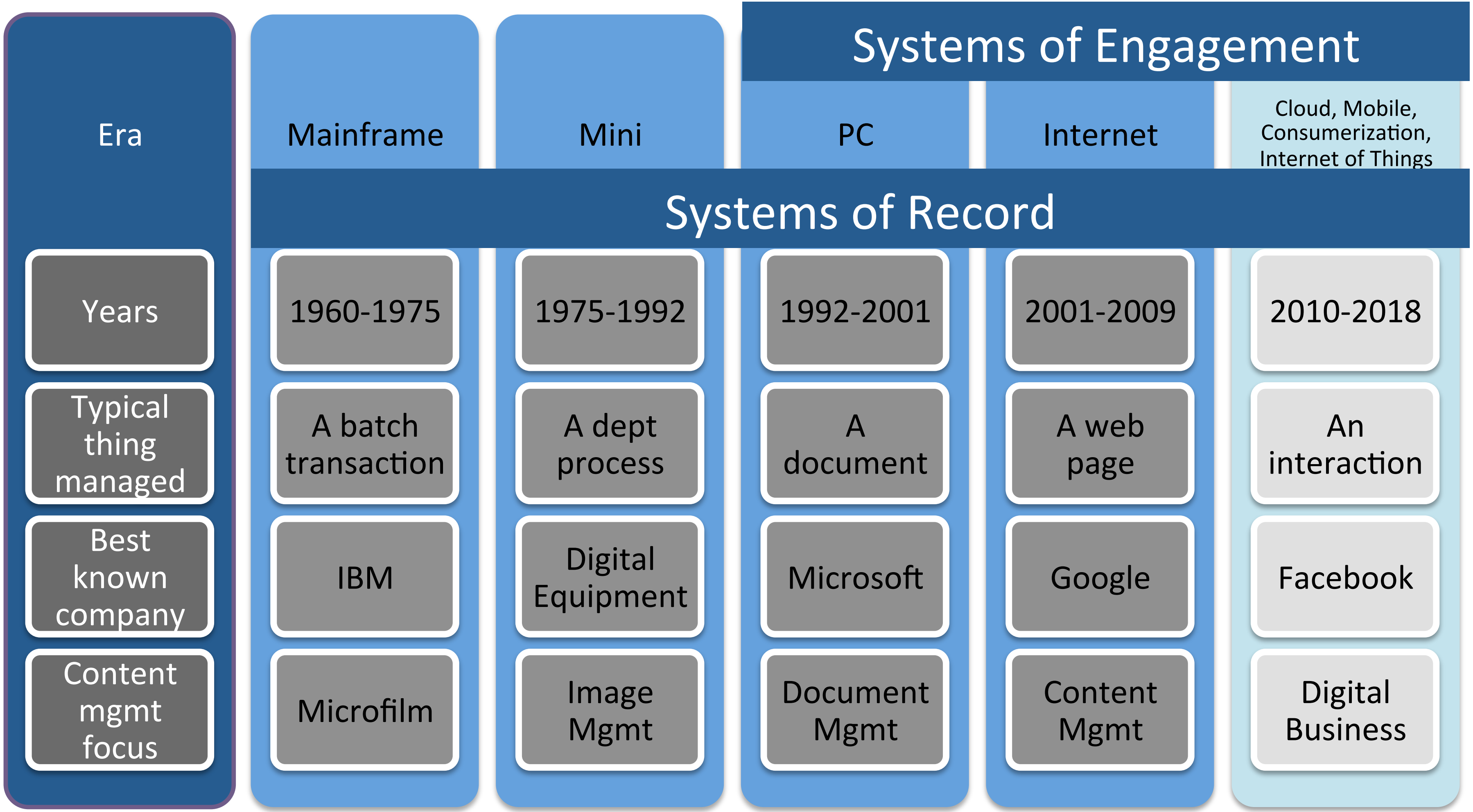
GDPR

How to Ensure Compliance?

Atle Skjekkeland, SVP, AIIM
@skjekkeland
askjekkeland@aiim.org



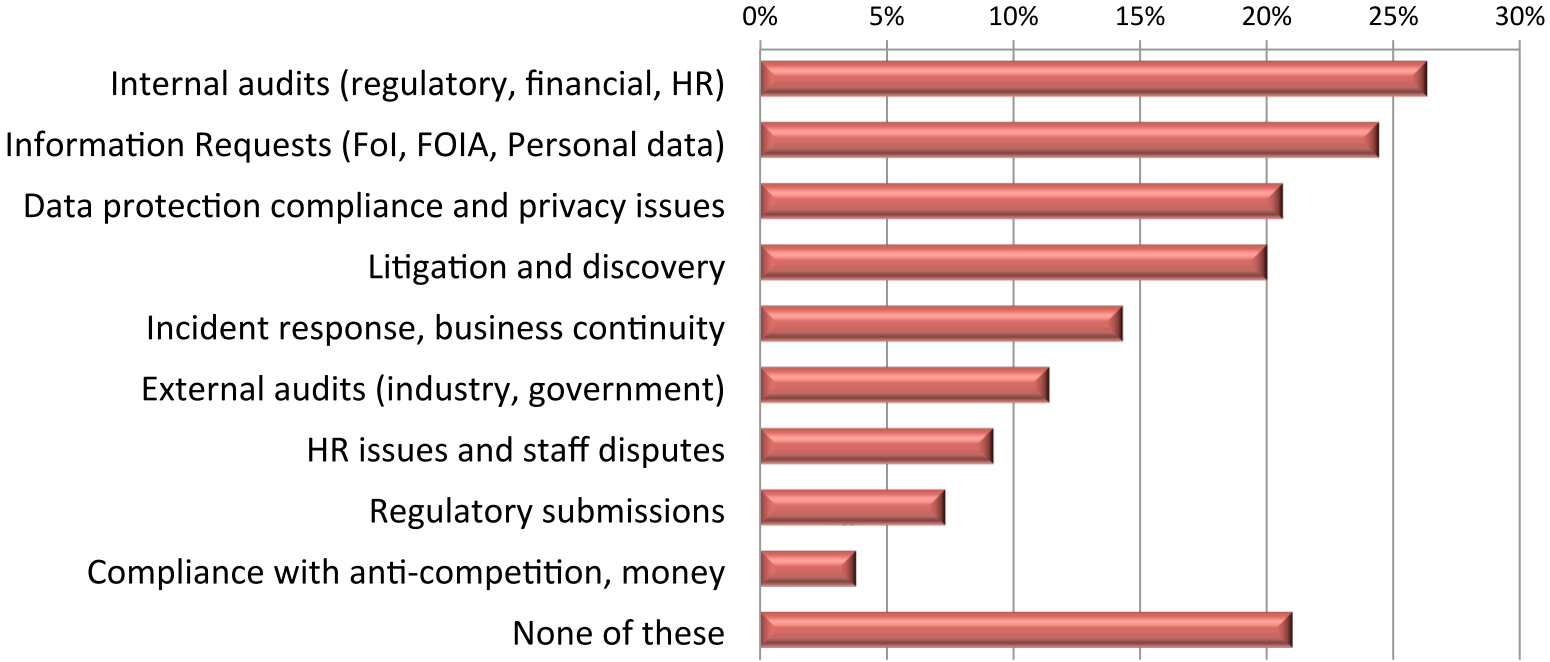
Systems of Engagement

Systems of Record

Era	Mainframe	Mini	PC	Internet	Cloud, Mobile, Consumerization, Internet of Things
Years	1960-1975	1975-1992	1992-2001	2001-2009	2010-2018
Typical thing managed	A batch transaction	A dept process	A document	A web page	An interaction
Best known company	IBM	Digital Equipment	Microsoft	Google	Facebook
Content mgmt focus	Microfilm	Image Mgmt	Document Mgmt	Content Mgmt	Digital Business

Compliance Risks

In your organization, has non-compliance with good Information Governance practice created a significant issue with any of the following in the last 2 years?



General Data Protection Regulation

- The **General Data Protection Regulation (GDPR)** (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the European Council and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU).
- It also addresses the export of personal data outside the EU.
- The primary objectives of the GDPR are to give citizens and residents back control of their personal data and to **simplify the regulatory environment for international business by unifying the regulation within the EU**.
- When the GDPR takes effect it will replace the data protection directive (officially Directive 95/46/EC) from 1995.
- **GDPR applies from 25 May 2018** after a two-year transition period and, unlike a directive, it does not require any enabling legislation to be passed by national governments.

Who Is It For?

- The regulation applies if the data **controller** (organisation that collects data from EU residents) or **processor** (organisation that processes data on behalf of data controller e.g. cloud service providers) or the data subject (person) is based in the EU.
- Furthermore the Regulation also applies to organisations based outside the European Union if they collect or process personal data of EU residents.

What Type of Information

According to the European Commission:

- “Personal data is any information relating to an individual, whether it relates to his or her private, professional or public life.”
- “It can be anything from a **name**, a **home address**, a **photo**, an **email address, bank details, posts on social networking websites, medical information,** or a **computer’s IP address**.”

Unstructured content is really important in relation with GDPR.

W
X
P
O
N
P
S
A
SharePoint
Dropbox
SAP
salesforce
WordPress

Sanctions

- A warning in writing in cases of first and non-intentional non-compliance.
- Regular periodic data protection audits.
- A fine up to **10,000,000 EUR** or up to **2% of the annual worldwide turnover** of the preceding financial year in case of an enterprise, whichever is greater (Article 83, Paragraph 4)).
- A fine up to **20,000,000 EUR** or up to **4% of the annual worldwide turnover** of the preceding financial year in case of an enterprise, whichever is greater (Article 83, Paragraph 5 & 6).

Personal Data Shall Be…

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('**lawfulness, fairness and transparency**');

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes… ('**purpose limitation**');

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('**data minimisation**');

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('**accuracy**');

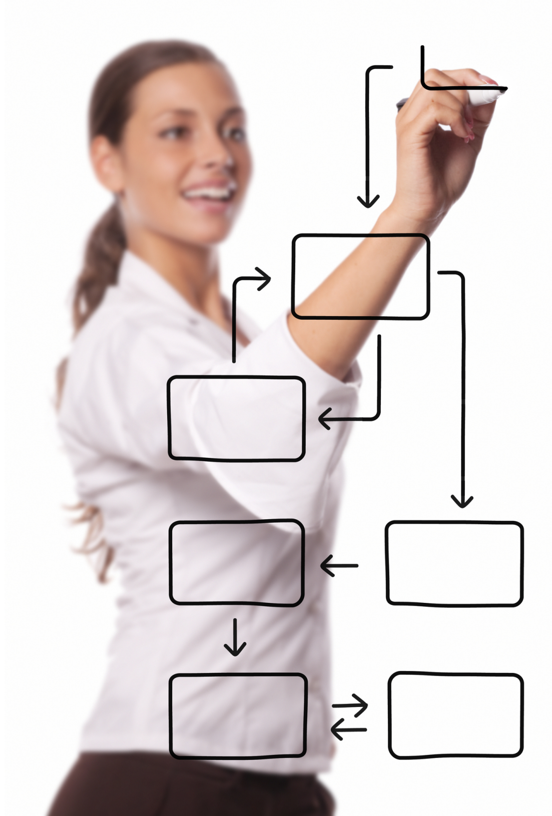
(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed…. ('**storage limitation**');

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('**integrity and confidentiality**').

Responsibilities

- In order to be able to demonstrate compliance with the GDPR, the data controller should implement measures which meet the principles of **data protection by design** and **data protection by default**.
- **Privacy by Design** and **by Default** (Article 25) require that data protection measures are designed into the development of business processes for products and services.
- **It is the responsibility and liability of the data controller to implement effective measures and be able to demonstrate the compliance of processing activities even if the processing is carried out by a data processor on behalf of the controller**. (Recital 74).
- Data Protection Impact Assessments (Article 35) have to be conducted when specific risks occur to the rights and freedoms of data subjects.

Privacy by Design and by Default



- **Privacy by Design and by Default** (Article 25) requires that data protection is designed into the development of business processes for products and services.
- This requires that privacy settings must be set at a high level by default, and that technical and procedural measures should be taken care by the controller in order to make sure that the processing, throughout the whole processing lifecycle, complies with the regulation.
- Controllers should also implement mechanisms to ensure that personal data is only processed when necessary for each specific purpose.

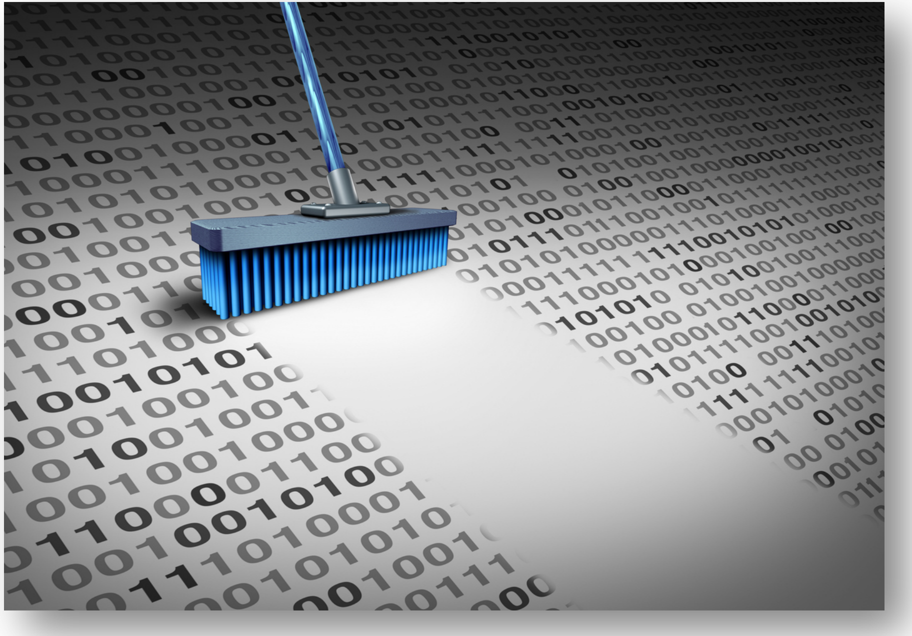
Consent

- Valid consent **must be explicit for data collected** and **the purposes data is used for** (Article 7; defined in Article 4).
- Consent for children must be given by the child’s parent or custodian, and verifiable (Article 8).
- Data controllers must be able to prove "consent" (opt-in) and consent may be withdrawn.

Pseudonymisation

- The GDPR refers to pseudonymisation as a process that transforms personal data in such a way that the resulting data cannot be attributed to a specific data subject without the use of additional information.
  - An example of pseudonymisation is encryption, which renders the original data unintelligible and the process cannot be reversed without access to the right decryption key.
  - The GDPR requires that this additional information (such as the decryption key) be kept separately from the pseudonymised data.
  - Pseudonymisation is recommended to reduce the risks to the concerned data subjects and also help controllers and processors to meet their data-protection obligations (Recital 28).
  - If the personal data is pseudonymised with adequate internal policies and measures by the data controller, then it is considered to be effectively anonymized, and not subject to controls and penalties of the GDPR.
  - The policies and measures that meet the principles of data protection by design and data protection by default should be considered adequate for this purpose.
  - Example measures would include pseudonymizing the data as soon as possible (Recital 78), encrypting the data locally, keeping the decryption keys separately from the encrypted data.

Right to Erasure



- Article 17 provides that the data subject has the right to request erasure of personal data related to them on any one of a number of grounds including non-compliance with article 6.1 (lawfulness) that includes a case (f) where the legitimate interests of the controller is overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data

Data Portability

- A person shall be able to transfer their personal data from one electronic processing system to and into another, without being prevented from doing so by the data controller.
- In addition, the data must be provided by the controller in a structured and commonly used electronic format.
- The right to data portability is provided by Article 20 of the GDPR.

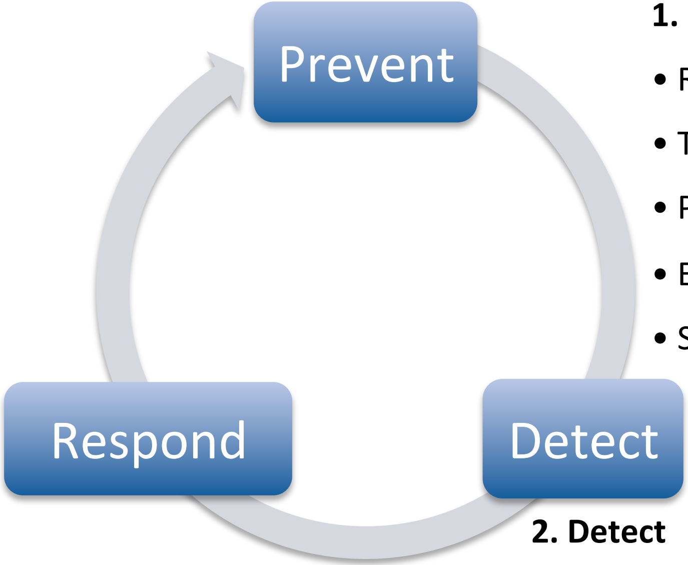
Data Breaches

- Under the GDPR, the Data Controller will be under a legal obligation to notify the Supervisory Authority without undue delay.
- The data breach must be reported to the Supervisory Authority within 72 hours of the data breach (Article 33).
- Individuals have to be notified if adverse impact is determined (Article 34).
- However, the data processor or controller do not have to notify the data subjects if anonymized data is breached.
- Specifically, the notice to data subjects is not required if the data controller has implemented pseudonymisation techniques like encryption along with adequate technical and organizational protection measures to the personal data affected by the data breach (Article 34).

7 Steps to GDPR Compliance

1. Identify use of personal data and content to ensure **lawfulness, fairness and transparency**
2. **Limit purpose** and **data minimization** by only collecting information for specified, explicit and legitimate purposes
3. Connect data and content to get a unified view for better control, portability, and deletion
4. Use metadata to ensure privacy-by-design and by default compliance
5. Apply retention management to **limit storage**
6. Use encryption at transit and at rest to ensure **integrity and confidentiality**
7. Use access control lists, permission management, and audit trails to ensure compliance

Establish a Compliance Framework



1. Prevent

- Risk assessments
- Training
- Policies & procedures
- Executive commitment
- Systems

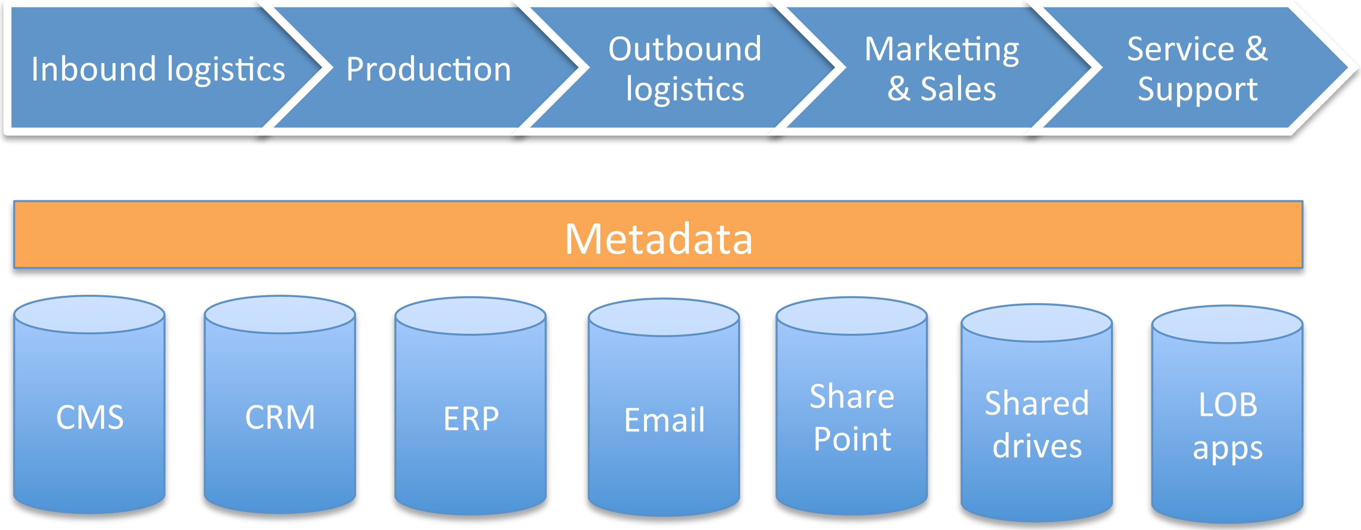
2. Detect

- Data Protection Officer
- Audit
- Monitoring

3. Respond

- Reporting
- Investigation
- Communication
- Improvements
- Employee discipline

Establish Privacy by Design/Default



Metadata extraction and metadata management is key for managing unstructured content in relation with GDPR.

Keep IT Simple and Smart

"Organizational culture eats strategy for breakfast, lunch and dinner" – **Peter Drucker.**

New IT:

Old IT: