Audit of GDPR Readiness

GDPR from an Internal Audit perspective

IIA Norway, 25 January 2018

Ole Svenningsen & Mounir Messaoud

First things first

The content, reflections and view points of this presentation represent the speakers' own and not necessarily those of their organisation.

Learning objectives

After the session you will gain a better understanding of:

- The role we have as auditors
- Key risk areas
- Governance needed
- Important elements
- Things to forget
- Things not to forget

Why audit GDPR readiness?

What are the key risk areas?

- Governance
- Data Management
- Training & Awareness
- Security
- Individual's rights
- International transfers & Third parties

Governance

Risk

- Without robust governance processes including data protection policies and procedures there is a risk that personal data may not be processed in compliance with the GDPR resulting in regulatory action and/or reputational damage.

Controls

- Data governance is appropriately managed across all roles and functions
- Clearly defined policies and procedures for data privacy are appropriately addressed for enterprise usage and guidance of personally identifiable information
- Assigned Accountability
- Data Protection or Privacy Programme

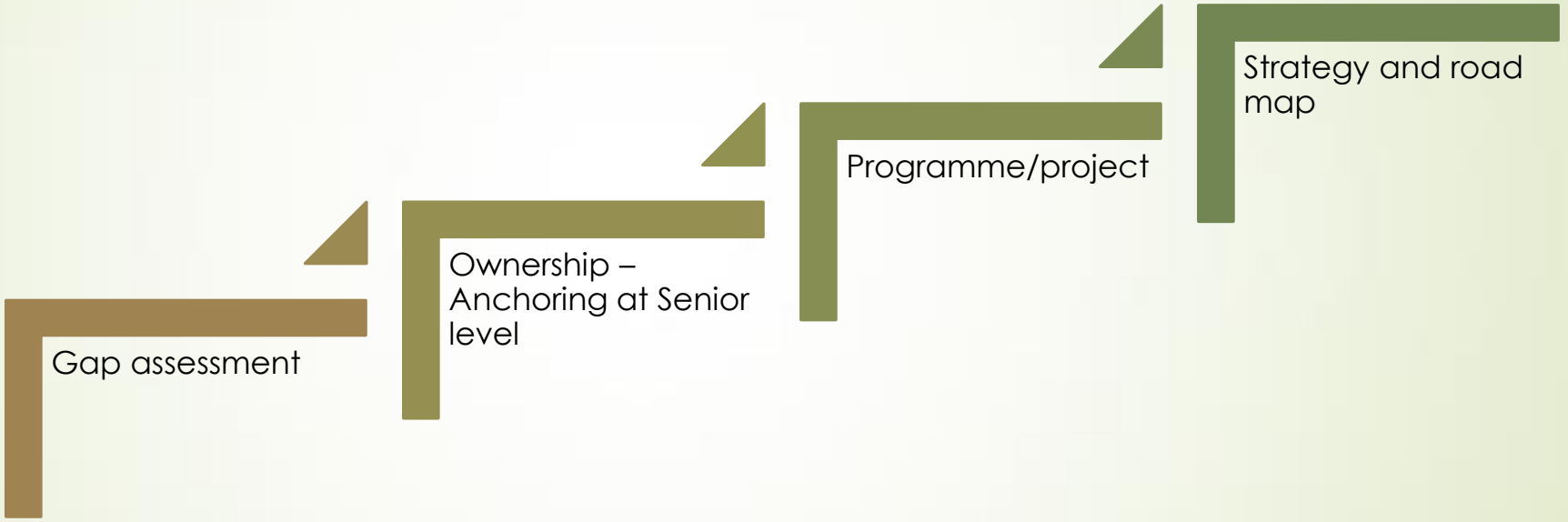
Evidences

- Policies
- Job Descriptions
- Organisational charts
- Business cases
- Steering Committee minutes
- Policy Communication plans and supporting instructions
- Management Risk Reports

Where to begin?

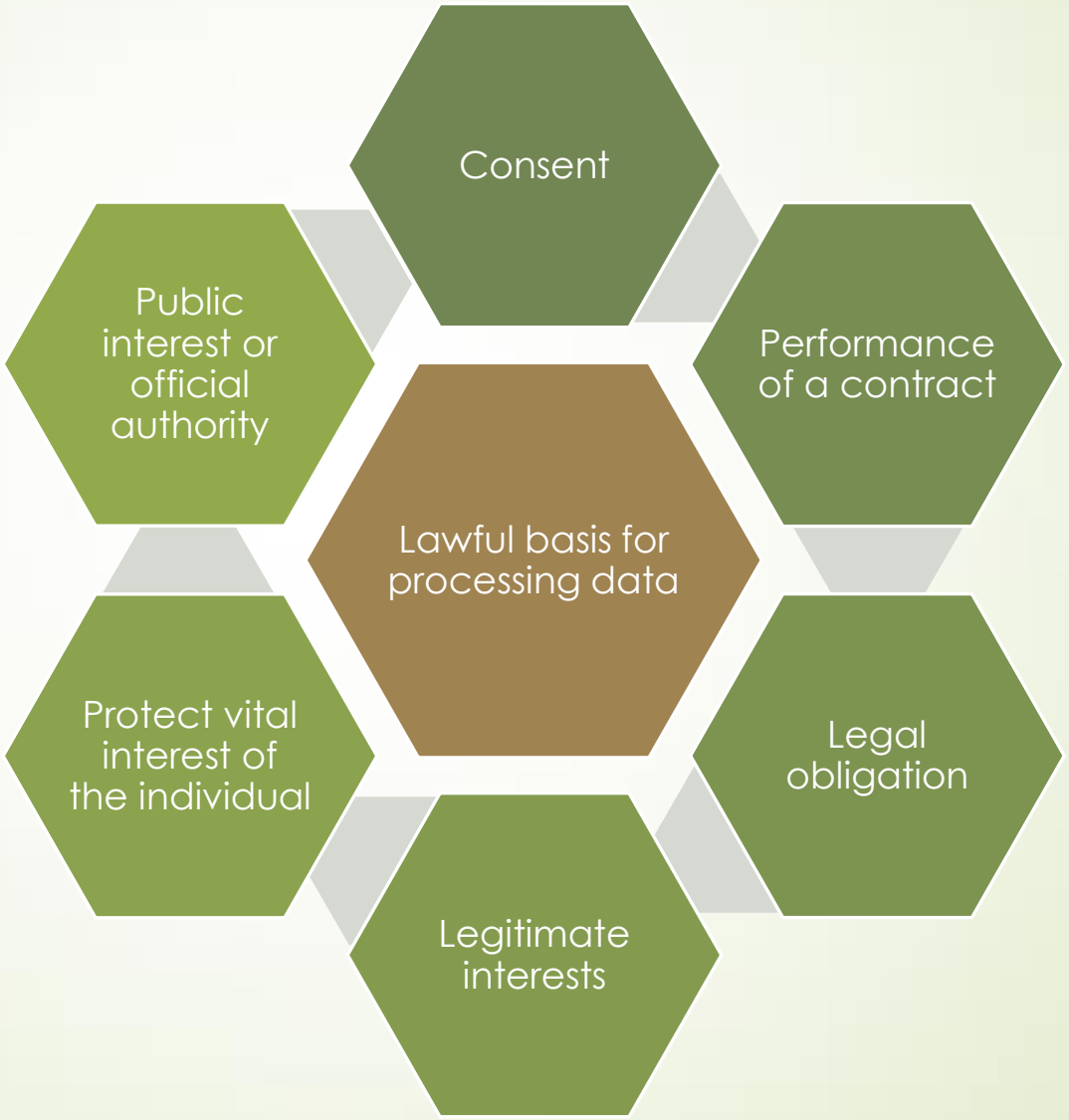
Selected key areas to consider in a readiness audit

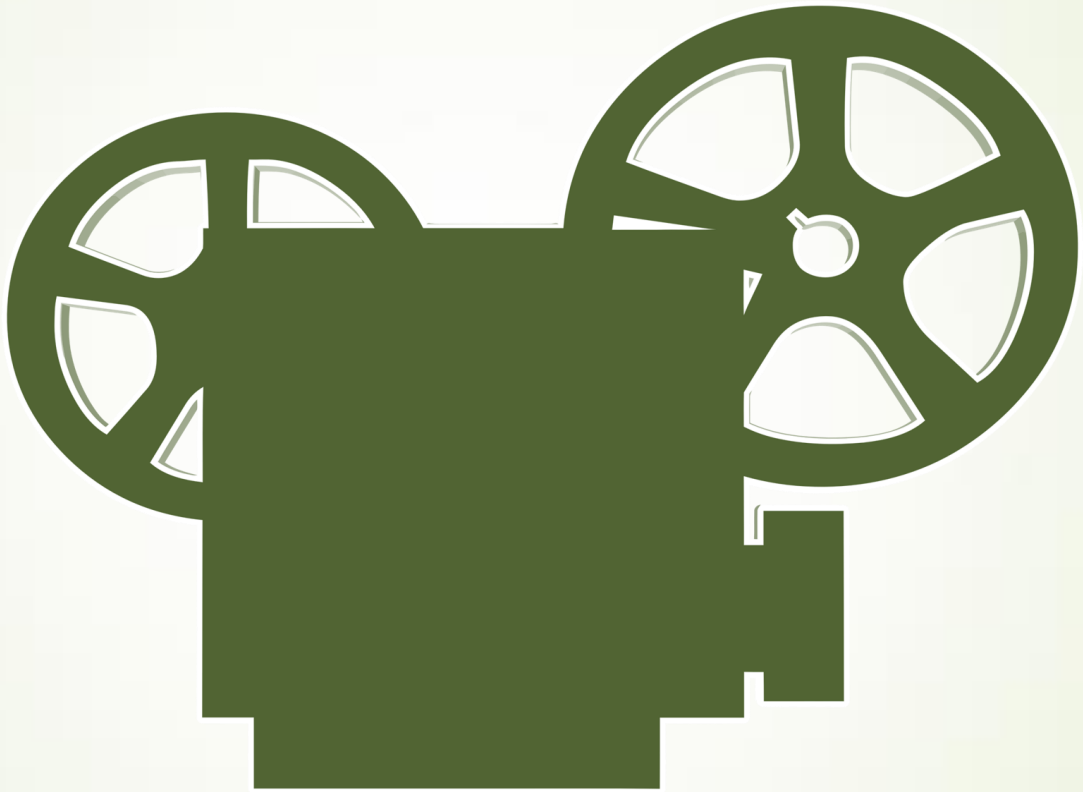
Understanding the GDPR



Data, data and data

Lawfulness of processing



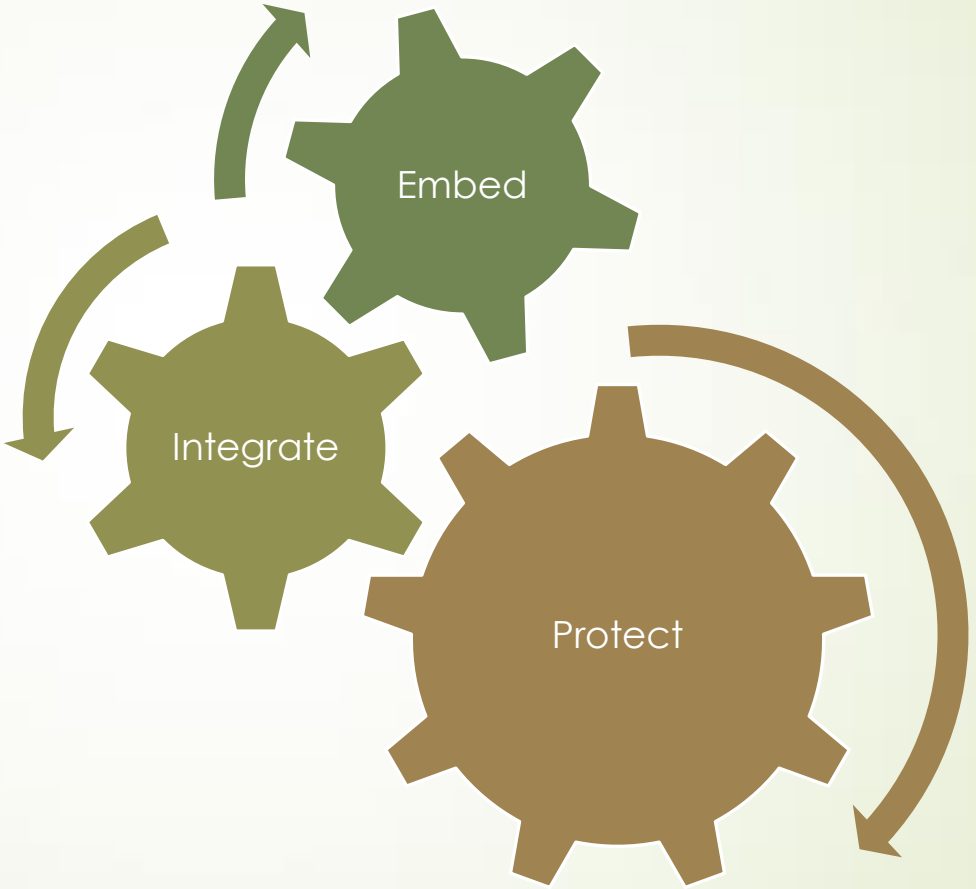


Individuals rights

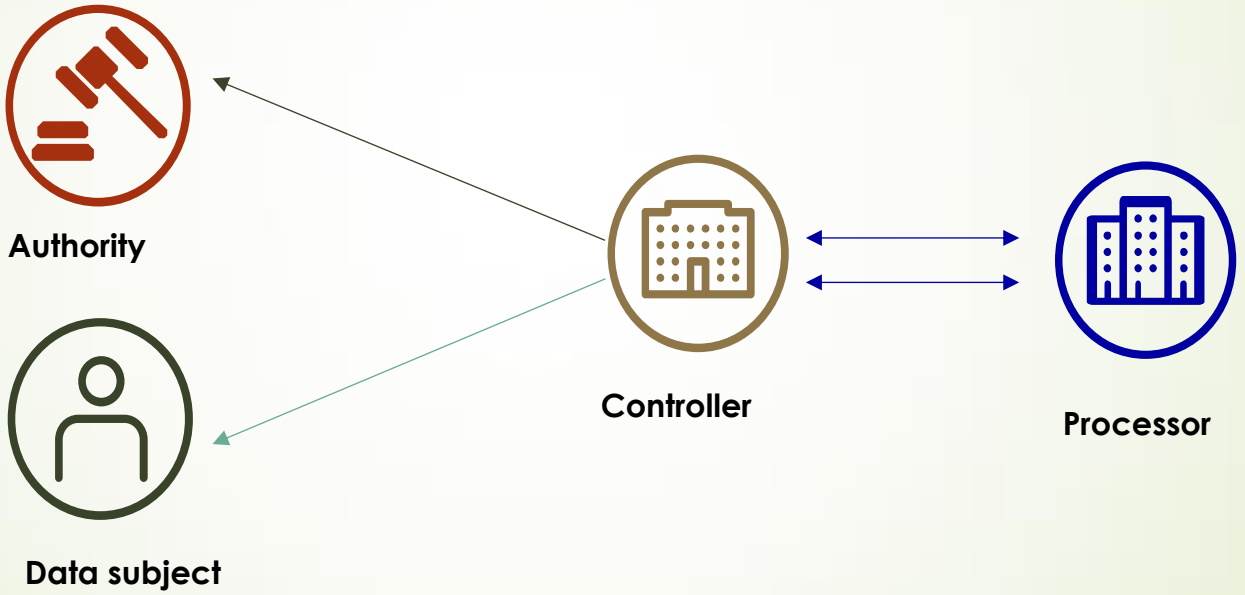
- The right to be informed
- The right of access
- The right to rectification
- The right to erasure ('right to be forgotten')
- The right to restrict processing
-The right to data portability
- The right to object

International transfers & third parties

Data Protection by Default and by Design



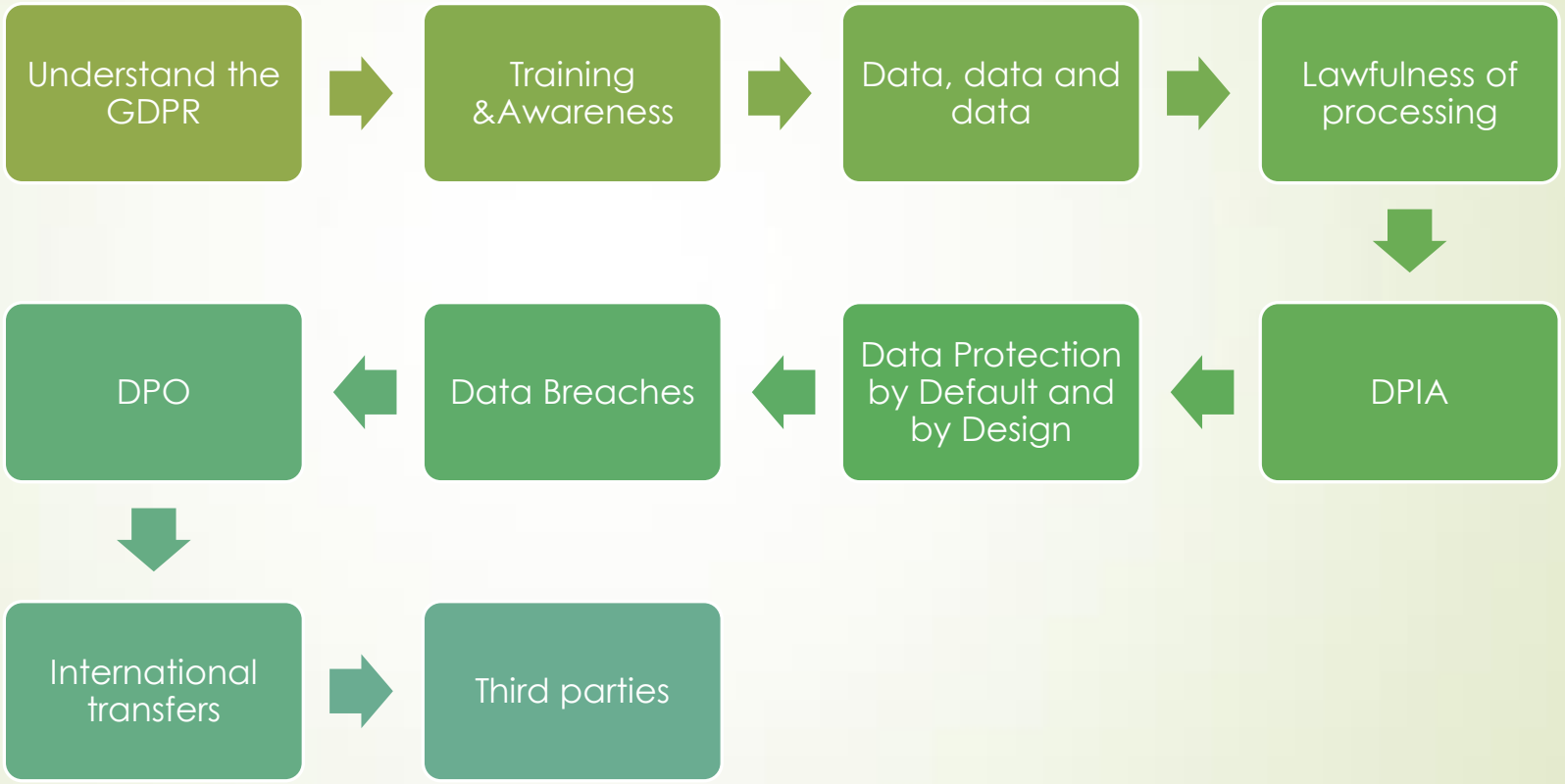
Breach and breach notification



http://www.computerweekly.com/news/252433538/Norwegian-healthcare-breach-alert-failed-GDPR-requirements

Accountability

Questions


Understand the GDPR
Training &Awareness
Data, data and data
Lawfulness of processing
DPIA
Data Protection by Default and by Design
Data Breaches
DPO
International transfers
Third parties

Contact Us

Ole Svenningsen

Head of Audit Group Functions IT

ole.svenningsen@nordea.com

www.linkedin.com/in/osven/

Mounir Messaoud

Internal Audit Manager

mounir.messaoud@nordea.com

www.linkedin.com/in/mounirmessaoud