GDPR

Jochen Nickel | inovit GmbH
Solution Architect
@jochennickel
https://www.inovit.ch

Protection of personal data

The **General Data Protection Regulation** (GDPR) imposes new rules on organizations that offer goods and services to people in the European Union (EU), or that collect and analyze data tied to EU residents, no matter where they are located.

- **Enhanced** personal privacy rights
- **Increased** duty for protecting data
- **Mandatory** breach reporting
- **Significant** penalties for non-compliance

Personal privacy

Individuals have the right to:

- Access their personal data
- Correct errors in their personal data
- Erase their personal data
- Object to processing of their personal data
- Export personal data

Controls and notifications

Processors will need to:

- Protect personal data using appropriate security practices
- Notify authorities within 72 hours of breaches
- Receive consent before processing personal data
- Keep records detailing data processing

Transparent Policies
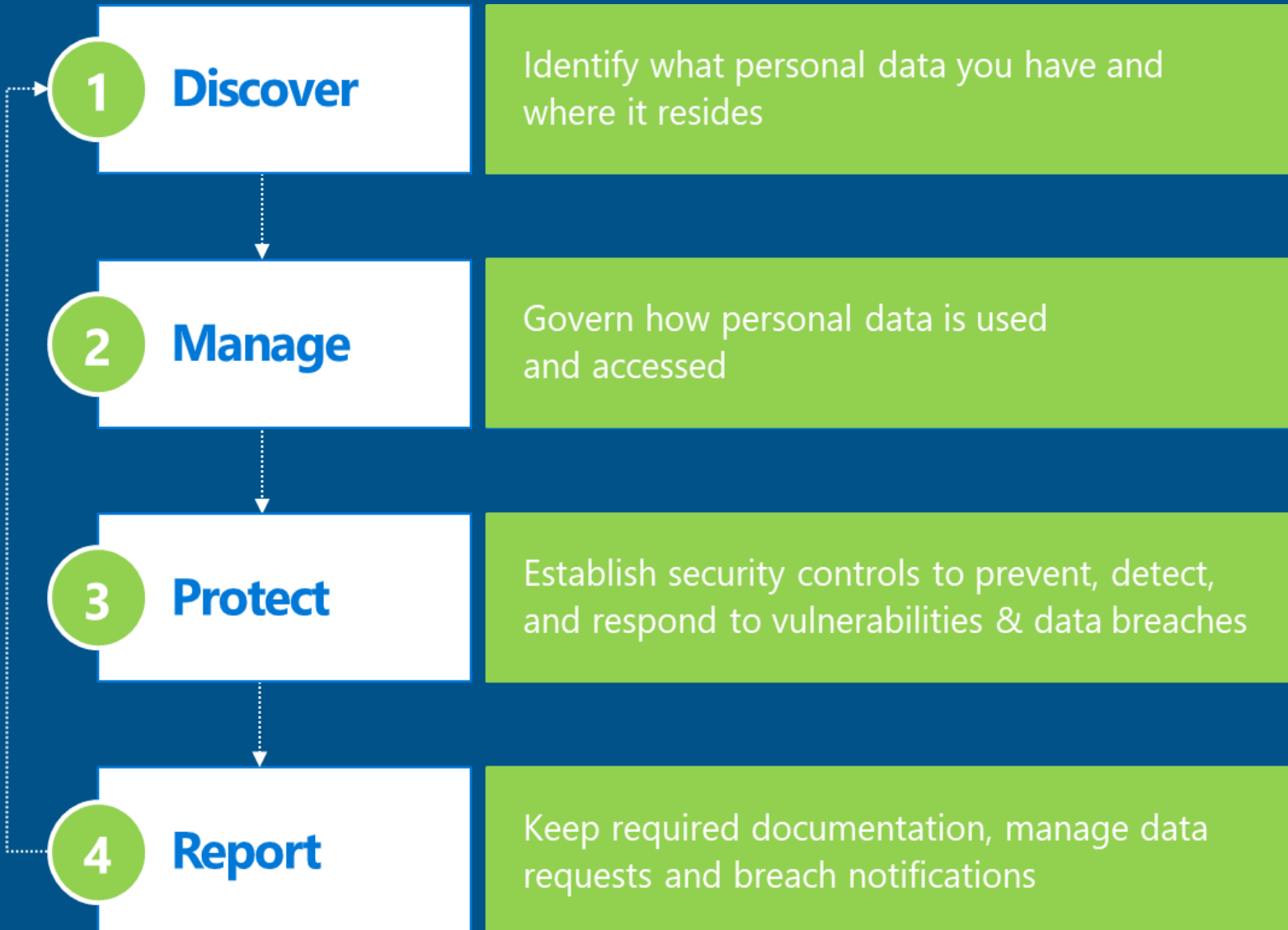
Processors are required to:

- Provide clear notice of data collection

- Outline processing purposes and use cases

- Define data retention and deletion policies

IT and Training

Processors will need to:
- Train privacy personnel & employee
- Audit and update data policies
- Employ a Data Protection Officer (for larger organizations)
- Create & manage processor/vendor contracts

Get ready for GDPR

1 Discover
Identify what personal data you have and where it resides

2 Manage
Govern how personal data is used and accessed

3 Protect
Establish security controls to prevent, detect, and respond to vulnerabilities & data breaches

4 Report
Keep required documentation, manage data requests and breach notifications

Relevant articles

Art. 7, Sec. 3
Art. 9
Art. 15 & 20
Art. 25, Sec. 1
Art. 25, Sec. 2
Art. 30
Art. 32, Sec. 1
Art. 33
Art. 46, Sec. 1
Art. 46, Sec. 2-3

Discover

- Any data that helps you identify a person
  - Name, Email address, Social media posts, Location
  - Medical information, Physical, physiological, or genetic information
  - Bank details, IP address, Cookies, Cultural identity
- Identifying where personal data is collected and stored
  - Emails, Documents, Databases, Removable media
  - Metadata, Log files, Backups

Manage

- Defining policies, roles and responsibilities for the management and use of personal data
  - At rest, In process, In transit
  - Storing, Recovery
  - Archiving, Retaining, Disposal
- Organizing and labeling data to ensure proper handling
  - Types, Sensitivity, Context / use
  - Ownership, Custodians, Administrators, Users

Protect

- Protecting your data
  - Physical datacenter protection, Network security, Storage security
  - Identity management, Access control, Encryption
  - Compute security, Risk mitigation
- Monitoring for and detecting system intrusions
  - System monitoring, Disaster recovery
  - Breach identification, Notifying DPA & customers
  - Calculating impact, Planned response

Report

- Enterprises will need to record the:
  - Purposes of processing, Classifications of personal data
  - Third-parties with access to the data, Data retention times
  - Organizational and technical security measures
- Implement reporting capabilities
  - Cloud services (processor) documentation, Audit logs
  - Breach notifications, Handling Data Subject Requests
  - Governance reporting, Compliance reviews

Many thanks!