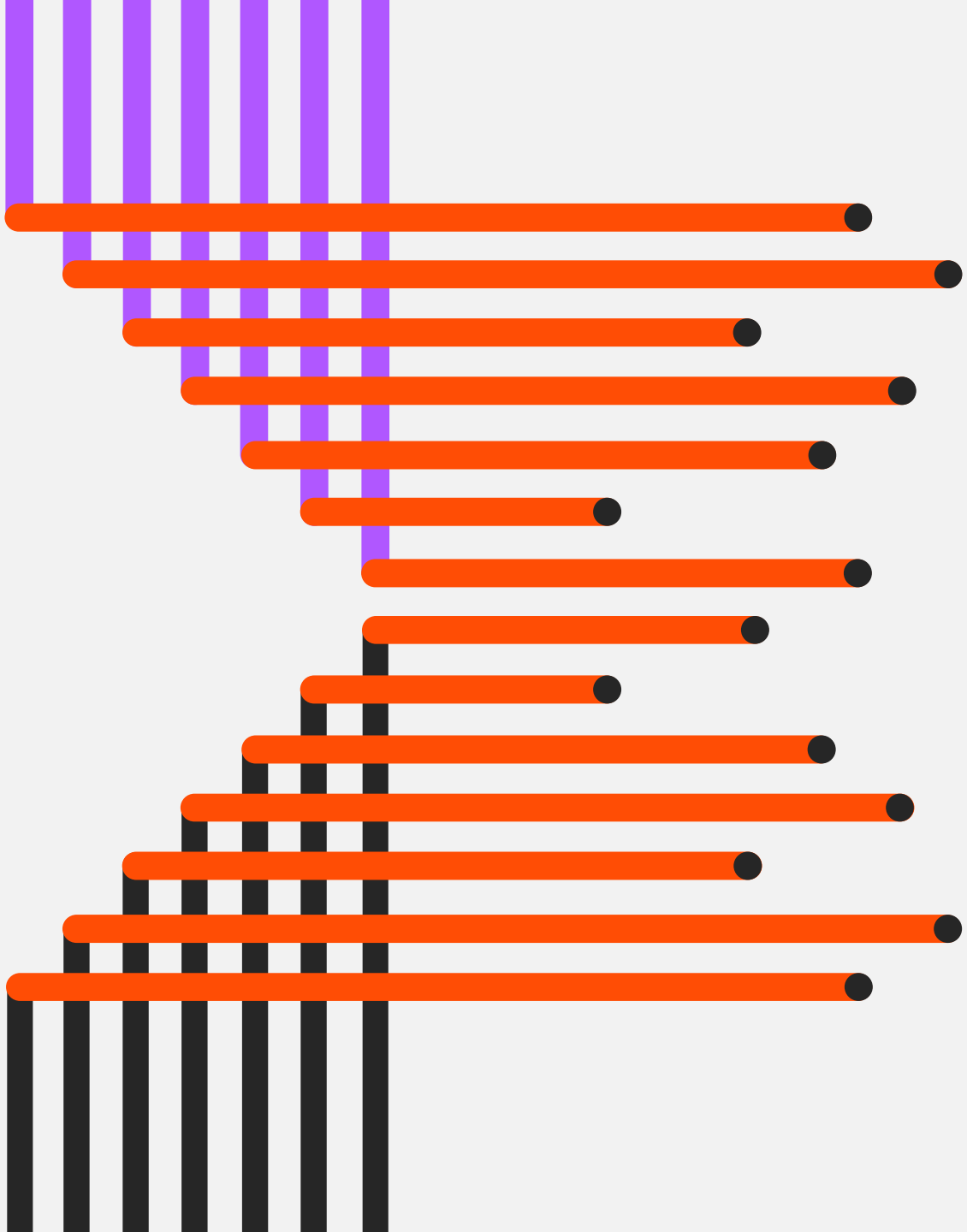


Privacy by Design

Keynote @ Digital Era

Riga 2018-05-25

Margaretha Eriksson

Digital Trust, Acando Consulting AB

margaretha.eriksson@acando.com

It is about Margaretha

Margaretha Eriksson

M.Sc. E.E. Royal Institute of Technology (KTH), Stockholm, Sweden

GDPR and Cyber Security Expert at Digital Trust, Acando Consulting AB Stockholm, Sweden

IEEE Senior Member

Advisor to IEEE CIO on GDPR

IEEE Director for EMEA (Region 8)

It is about GDPR article 25

The controller shall, both at the time of determination of the **means for processing** and at the **time of** the **processing** itself, implement appropriate **organizational and technical measures** which are designed to **implement data-protection principles** to integrate safeguards into the processing in order to be compliant with GDPR.

The controller shall implement appropriate **technical and organizational measures** for ensuring that, by default, **only personal data necessary** for each **specific purpose** of the processing are processed.

It is about the Security Requirements

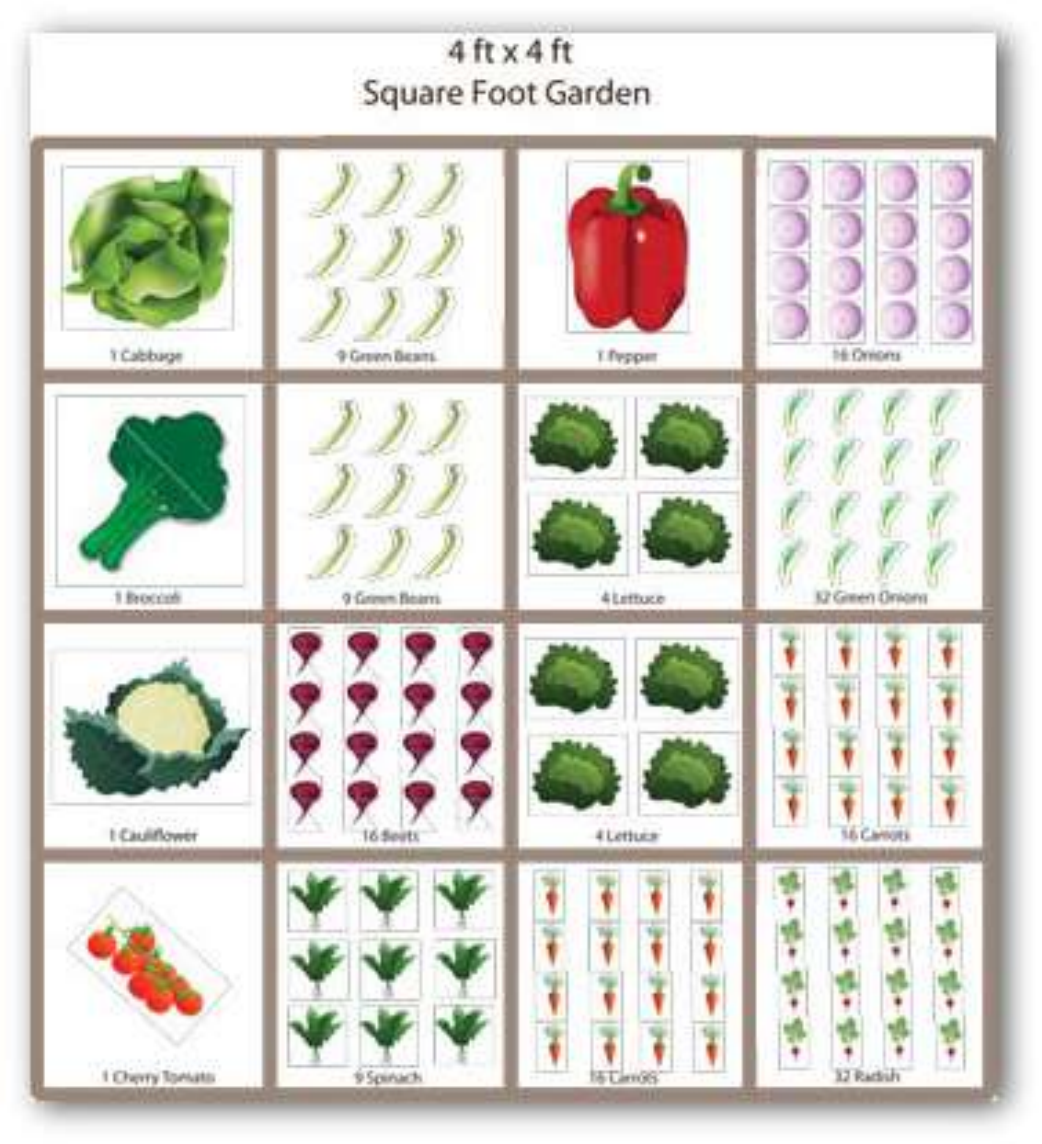
Guidelines should provide guidance regarding **security requirements** to be applied to products

Requirements should be **aligned** with the organization's **regulatory framework** and relevant **standards** regarding **information security** and **GDPR**

- ISO 27001 - Information technology - Security Techniques - Information security management systems — Requirements
- ISO 27002 - Code of practice for information security controls
- ISO 29151 - Code of practice for personally identifiable information protection
- ISO 29134 - Guidelines for privacy impact assessment

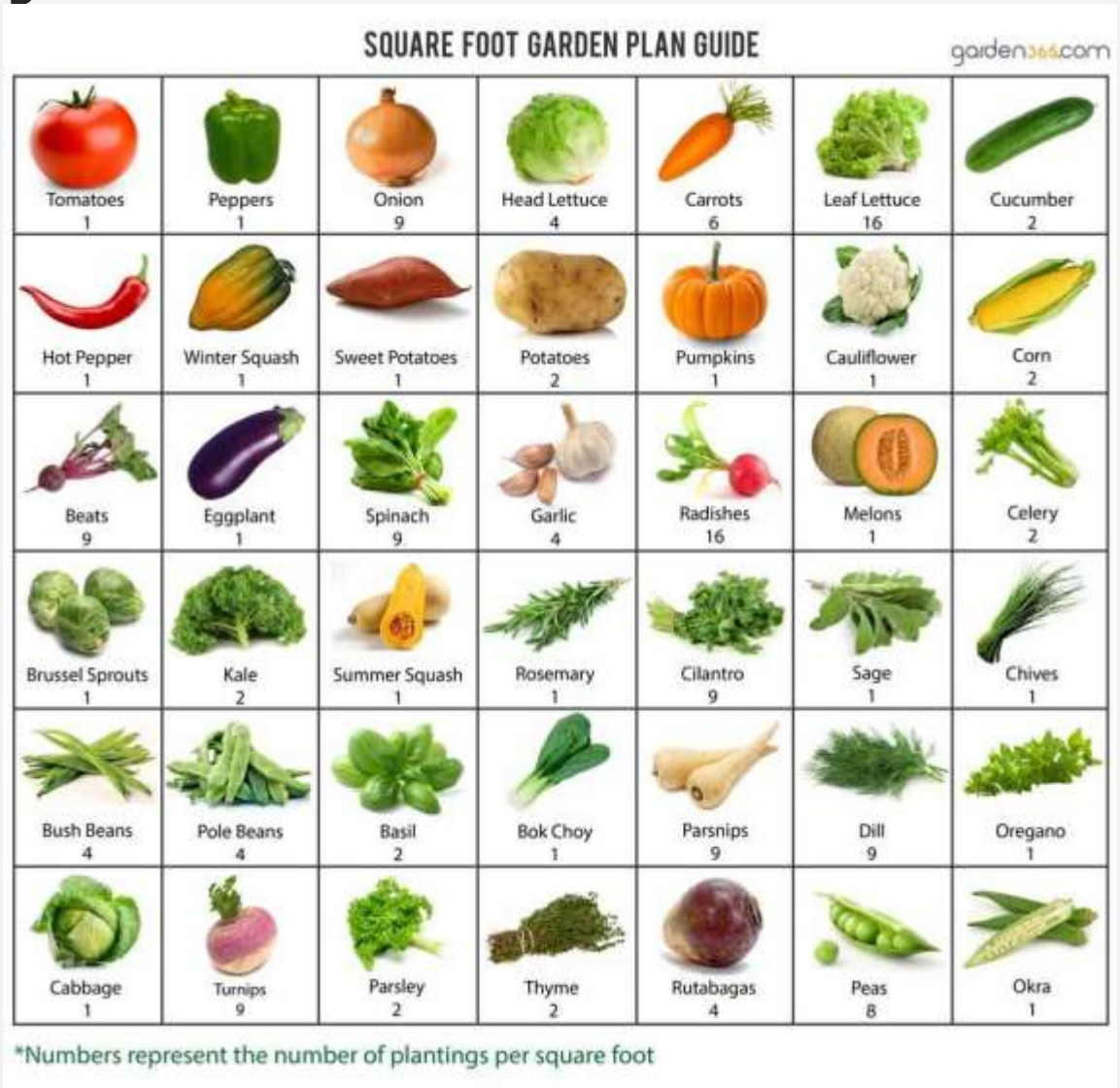
It is about the use of Personal Data

- The purpose of using Personal data
- Confidentiality of Personal data
- Integrity of Personal data
- Availability
- Accuracy



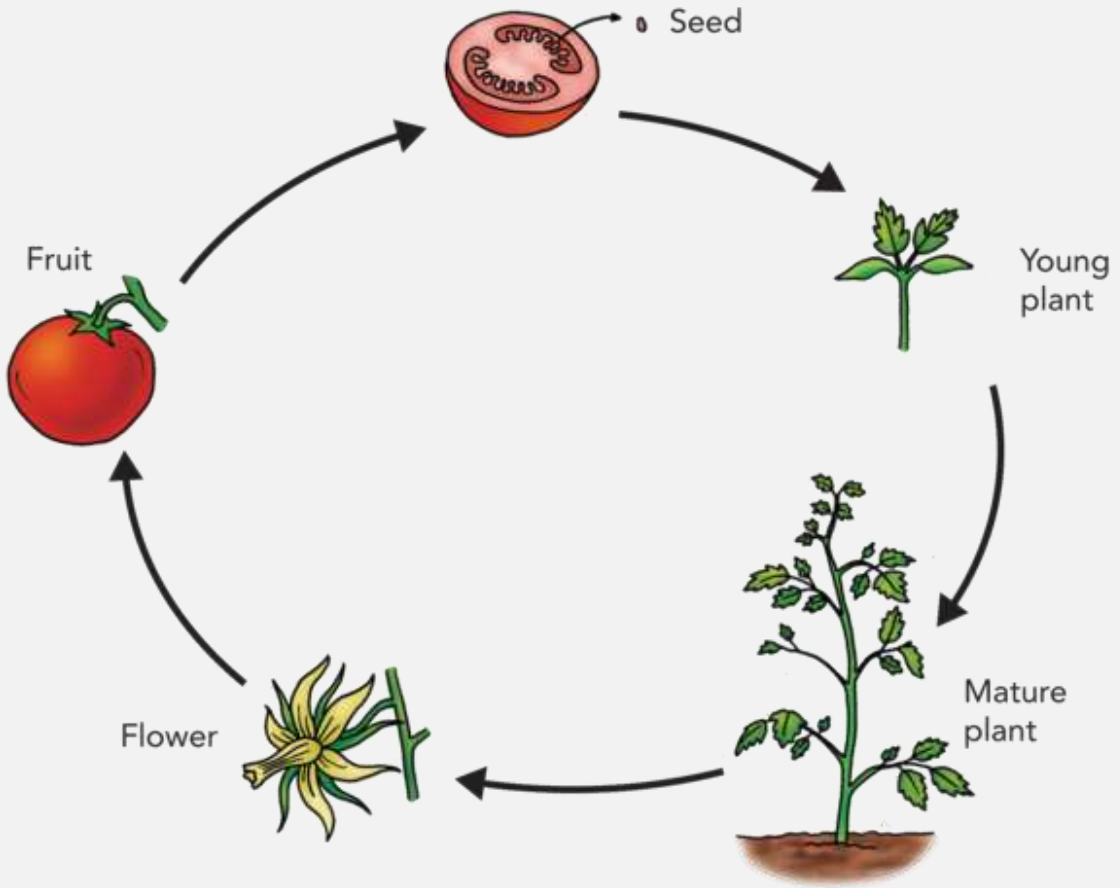
It is about the Project

- Set proper Privacy Requirements
- Build in Security functions



It is about the Life Cycle of Data

- Collect only the data you need (Not more!)
- Which personal data do you need?
- Save data as long as you need (Not longer!)
- Clean out data when due (Don’t save forever!)
- Clean out personal data from mail boxes and storages



It is about Education

- Educate everybody on how to work with Personal data
  - Management
  - IT personell
  - Users
  - Project Managers
  - IT Architects
  - Coders
  - Stakeholders…

It is about Communication

- Translate the GDPR legal words into real world messages
- Explain why it is important to handle personal data with care
- Talk about the cost of sanctions and how to avoid it
- ”Be a Duck”!

It is about System Maintainance

- Can the system be adapted to comply with Privacy by Design requirements?
- Can the system be phased out?
- Can we add a supporting process to be compliant?


DIGITAL
era
2018
GDPR