GDPR Projects – cases & examples
Nordic GRC Summit, 15 March 2017
Tim Clements CIPP/E, CIPM, CIPT, CRISC, CGEIT
Scope of this presentation

- The GDPR project – a new paradigm?
- Falck’s GDPR project – approach & structure
- Identifying GDPR project scope
- Identifying data flow scope
- Data flow mapping – an approach
- Ensuring ongoing compliance
- The human factor
- A slide for the busy executives
Scope of this presentation

- The GDPR project – a new paradigm?
- Falck’s GDPR project – approach & structure
- Identifying GDPR project scope
- Identifying data flow scope
- Data flow mapping – an approach
- Ensuring ongoing compliance
- The human factor
- A slide for the busy executives
GDPR Project

“When eating an elephant take one bite at a time”
*Creighton W. Abrams*

“You people are telling me what you think I want to know. I want to know what is actually happening”

“They've got us surrounded again, the poor bastards”
GDPR Project

How compliant are you with existing data protection legislation?

GDPR – a “bit extra” on top of an existing regime

GDPR – a new recipe may be needed
GDPR – just another compliance project!

The journey:

Today

Identify the key Data Protection risks

Treat the key risks

Establish the right level of governance across the organisation

Get the people ready (responsibilities, competences, mindset)

Deadlines from your B2B customers (?)

May 2018
Scope of this presentation

- The GDPR project – a new paradigm?
- Falck’s GDPR project – approach & structure
- Identifying GDPR project scope
- Identifying data flow scope
- Data flow mapping – an approach
- Ensuring ongoing compliance
- The human factor
- A slide for the busy executives
Project approach at Falck

Business Areas

Address the obvious gaps early

- Kick off & risk workshops
- Data flow mapping & GAP analysis
- GAP list
- Other areas to be addressed
- Privacy data inventory
- Analysis, control selection & prioritisation
- Controls
- People
- Process
- Tech
- Planning & implementation of controls

Group Project Team

Establish governance

- Data Privacy strategy & policies
- Define roles & responsibilities, trigger recruitment of DPO(s)
- Educate, train & inform
- Define processes for PIA, Incidents, monitoring & reporting
- Incident process
- Privacy data inventory
- PIA
- Monitoring & reporting

2017: Business as Usual

First time PIA

- Kick off workshops
- Conduct first PIA
- DPO(s)
Project organisation at Falck

Executive Project Board
- Meets quarterly, strategic focus

Project Steering Committee
- Meets monthly, operational focus

Reference Group
- Subject matter experts (IT Directors)

Group Project Manager

Group Project Team
- Subject matter experts (Risk, Security, Legal, Controlling)

FHC Business Lead
- Business process owners
- Application managers
- Subject matter experts

ASS Business Lead
- Business process owners
- Application managers
- Subject matter experts

EME Business Lead
- Business process owners
- Application managers
- Subject matter experts

FSS Business Lead
- Business process owners
- Application managers
- Subject matter experts

GF Business Lead
- Business process owners
- Application managers
- Subject matter experts

HR Lead
- Business process owners
- Application managers
- Subject matter experts

IT Core Services Lead
- Application managers
- Subject matter experts
Scope of this presentation

- The GDPR project – a new paradigm?
- Falck’s GDPR project – approach & structure
- **Identifying GDPR project scope**
- Identifying data flow scope
- Data flow mapping – an approach
- Ensuring ongoing compliance
- The human factor
- A slide for the busy executives
Project scope – how to start

How does GDPR impact these perspectives in your organisation?

New or amended processes, procedures and functions

Changes to, or new organisational roles & responsibilities, staffing levels, skills and culture

Changes to, or new technologies, tools, IT applications, IT infrastructure

New or changes to information, data, documents, reports, records, etc.

Contracts, Data Processor Agreements, Policies, Consent Records, Privacy Notices etc., etc.
Project scope – example

GDPR Articles 35, 36 and 83 and Recitals 84, 89-96

(1) Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

Data Protection Impact Assessment

- Define Process for Data Protection Impact Assessment
- Revise Business Case process
- Revise IT Change Process
- Revise M&A processes
- Revise ERM process
- Revise Project Management Model
- Identify other relevant processes where risk assessment is made & add privacy dimension
- Implement changes to impacted processes
- Conduct competency assessment for required DPIA skills & knowledge
- Identify owner of DPIA Process
- Source expertise to assist in training where relevant
- Produce training materials for DPIA process
- Conduct training needs analysis e.g. asset owners
- Revise training materials for other relevant processes and refresh training
- Communicate updates about changed processes
- Conduct overall awareness
- Determine repository needs for DPIAs
- Changes to Risk Acceptance database
- Changes to Business Case tracker
- Changes to CAB tools
- Template for DPIA
- Report & sign-off template
- DPIA closure records
- Metrics for DPIA
- Internal reporting
Deliverables breakdown (PBS)
## GDPR Deliverables Roadmap – example 1

<table>
<thead>
<tr>
<th>Prepare &amp; plan</th>
<th>Pilot</th>
<th>Assessment</th>
<th>Control implementation &amp; change management</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>2017 Q1</td>
<td>2017 Q2</td>
</tr>
<tr>
<td><strong>Jan</strong></td>
<td><strong>Feb</strong></td>
<td><strong>Mar</strong></td>
<td><strong>Apr</strong></td>
</tr>
<tr>
<td><strong>Project team</strong></td>
<td>Kick-off</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Core team training</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Functional</strong></td>
<td>Kick-off</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Initial</strong></td>
<td>commns.</td>
<td>&amp; training</td>
<td></td>
</tr>
<tr>
<td></td>
<td>materials</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Data flow</strong></td>
<td>mapping</td>
<td>procedure &amp;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>process &amp;</td>
<td>template</td>
<td></td>
</tr>
<tr>
<td><strong>Prepare &amp; plan</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Assessment</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Control implementation &amp; change management</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Process, procedure</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Organisation/People</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Tool</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Information, data, documents</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Core activity</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Steering Committee meetings</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### GDPR Deliverables Roadmap – example 2

<table>
<thead>
<tr>
<th>Planning &amp; analysis</th>
<th>Assessment</th>
<th>Control implementation &amp; change management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apr 2016 Q2</td>
<td>Q3</td>
<td>Q4</td>
</tr>
<tr>
<td>Apr</td>
<td>May</td>
<td>Jun</td>
</tr>
<tr>
<td>DPO role reqts.</td>
<td>DPMS tool reqts.</td>
<td>GAP analysis process &amp; template</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Group Project Team</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Project Team KO</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business Area</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business Team defined</td>
<td>Business Area Plan</td>
<td>Business Activity update plan</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Key Points:**
- **2016 Q2:**
  - Data Flow mapping process & template
  - Training needs analysis
  - Mandate for Security/DP Board
- **2017 Q1:**
  - Data Flow mapping training materials
  - 1. training plan
  - DPMS tool
  - Privacy by design guidelines
  - DPO role in place

**Governance process implementation:**
- Risk Review (GAP analysis, identify key risks and control design)
- Risk Review (effectiveness of implementation)

**Privacy Data inventory:**
- Key Data Protection risks
- Business Activity update plan

**Project Management:**
- Data Protection Awareness
- Control implementation

**Roles processes & procedures updated:**
- DPO role in place
- Recruitment for needed competences

**Steering Committee meetings:**
- Roles

---

**Group Project Team:**
- Project Team KO

---

**Business Area:**
- Business Kick-off (top level)
- Business kick-off (process)

---

**Business org. Charts:**
- Application scope
- Business process scope

---

**Business Team defined:**
- Business Area Plan

---

**Process:**
- Organisation/People
- Technology
- Information
- Project Mgmt.
- Core activity

---

**Steering Committee meetings:**
- Roles

---

**Data Flow Mapping:**
- Data Flow Mapping (business processes)
- Data Flow Mapping (applications)
- Assess existing processes requiring amending
- Organisational competency assessment
- Recruit & training plan
- Role-specific training
- Recruitment for needed competences

---

**Data Protection Strategy:**
- Data Protection Policy
- Breach notif. procedure
- Customer activity processes

---

**Risk Review:**
- Effectiveness of implementation

---

**Control list:**
- Governance process implementation
- Risk Review (GAP analysis, identify key risks and control design)
- Risk Review (effectiveness of implementation)
Project scope – Deliverable Description

Data flow mapping procedure & template

Deliverable description

**Purpose**
- To consistently map the flow of personal data across the data life-cycle: collect/create, store, use, disclose, dispose in order to provide a basis for identifying compliance gaps and risks

**GDPR reference**
- To comply with the documentation requirements such as Article 30 (Records of processing activities), a number of items have to be documented after identifying personal data flows through drawing the diagrams.
- The documentation can also document potential risk and indicate compliance with a number of areas in the GDPR such as Articles* 5, 22, 24, 25, 30 and 32

*9: Principles relating to processing of personal data; 22: Automated individual decision making, including profiling; 24: Responsibility of the controller; 25: Data protection by design and by default; 30: Records of processing activities; 32: Security of processing

**Description and format**
The procedure will describe how to map the flow of personal data using standard procedure templates. The procedure will describe various elicitation approaches as well as how to complete the mapping template.

Completing the procedure will determine what data are collected, the reasons for collection, what the data is used for, how it is processed in each step (shared, edited, stored etc.), who has access to the data, is the data shared with other parties, is data used for other purposes than initially planned, role (controller, processor or both), are data processor agreements in place, does data flow outside the EU, etc.

The format of the template will be in Visio using vertical swim lanes for each stage of the data cycle.

**Owner**

**Due**
- January 2017

**Key tasks**

<table>
<thead>
<tr>
<th>Resource</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

**Dependencies**
- None

**Sign-off responsible**

-
Challenges & blessings at Falck

Data typically follows this lifecycle:

- Data is collected
- Data is stored
- Data is used
- Data is shared
- Data is disposed

System classification and application lists will help understand the initial scope

The need to understand where the key risks are in the data flows and ensure controls are in place

<table>
<thead>
<tr>
<th>Availability</th>
<th>Business critical</th>
<th>Critical</th>
<th>Less Critical</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criticality/integrity</td>
<td>Business Critical</td>
<td>Critical</td>
<td>Less Critical</td>
</tr>
</tbody>
</table>

- Applications
- Infrastructure
- Interfaces
- Partners
- Customers
- Suppliers etc.
Scope of this presentation

- The GDPR project – a new paradigm?
- Falck’s GDPR project – approach & structure
- Identifying GDPR project scope
- **Identifying data flow scope**
- Data flow mapping – an approach
- Ensuring ongoing compliance
- The human factor
- A slide for the busy executives
Identifying personal data scope
– key steps

1. Understand the definition of personal data & how this applies in your organisation
2. Review your organisation’s value chain or process overview (if available). Alternatively produce own overview to provide context
3. Identify data flows containing personal data using the 3-tier model as the context
4. Register data flows in Data Flow Scope Document and set prioritization criteria

Tools

- Data Flow Scope Decision Tree
- Value chain map
- 3 layer model
- Data Flow Scope Document guidance
- Data Flow Scope Document (Excel)
- Examples of Personal Data Identifiers
- Overview of processes
- EU GDPR definitions
### Data Flow Scope Decision Tree

**Is your Business Unit targeting services to EU member states, or processing, or have access to EU citizen data (incl. employee data)?**

- **No**
  - Document justification for decision and list applicable local data protection legislation
  - Out of GDPR scope

- **Yes**
  - What type of data is being processed or accessed in your business process or supporting application?
    - Non-personal data
      - Data not relating to any identifiable persons, out of scope for the GDPR project
      - Out of GDPR scope
    - Personal data*
      - Any information relating to an identified or identifiable natural person, i.e. someone who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Examples include: name, address, occupation, phone number, email address, online identifiers such as IP addresses & RFID tags, license plates, photos of named individuals, social security numbers, identification number, or other unique identifiers.
      - Add processes and/or applications to “in scope” list
      - Out of GDPR scope
    - Sensitive personal data*
      - Special categories of personal data revealing physical or mental health, trade-union membership, sex life or sexual orientation, racial or ethnic origin, political opinions, religious or philosophical beliefs, genetic or biometric data, administrative sanctions, judgments, criminal or suspected offences, convictions.
      - Add processes and/or applications to “in scope” list
Examples of Personal data identifiers
The idea of the value chain is based on the process view of organisations, the idea of seeing a manufacturing (or service) organisation as a system, made up of subsystems each with inputs, transformation processes and outputs.

In the GDPR Project, the Value Chain Map provides a useful context of identifying data flows containing personal data.
Overview of processes

- Generic HR example
Identifying data flow scope (conceptual)

A process can be supported by one or more applications.

An application (in-house or 3rd party) can support one or more processes.

Register in scope document (Excel)
Where to register data flow scope

<table>
<thead>
<tr>
<th>Scope</th>
<th>Data type</th>
<th>Title</th>
<th>Accountable</th>
<th>Responsible</th>
<th>Volume (records)</th>
<th>Risk (existing practices)</th>
<th>Interfaces</th>
<th>Criticality</th>
<th>Comment</th>
</tr>
</thead>
</table>

Register the **Title** of the data flow, process, application, infrastructure component etc. Be specific and ensure others will understand the title.

Register the names of the individuals who are **Accountable** and **Responsible** for the data flow or application. The Accountable person is typically the person with budget responsibility and the Responsible person(s) are people who take care of more day-to-day matters. In some cases this may be the same person.

State the approximate number of records that are collected, stored, processed, etc. in the data flow per year.

State your assessment of the complexity of interfaces between the data flow or application and other flows or applications.

Select the criticality the data flow or application has in terms of business activities.

State a risk category (**high**, **medium**, **low**) for the data flow – this is relevant if it is known that the existing practice may be close to being non-compliant.

Add any other information that may be relevant to the project team.

**Select** **In**, **Out** (or **Unsure**). It is deemed good practice to also register what is known not to be in-scope.

Select **Non-personal**, **Personal data** or **Sensitive personal data** using the definitions and examples.
Scope of this presentation

• The GDPR project – a new paradigm?
• Falck’s GDPR project – approach & structure
• Identifying GDPR project scope
• Identifying data flow scope
• **Data flow mapping – an approach**
• Ensuring ongoing compliance
• The human factor
• A slide for the busy executives
Data Flow Diagram – key concepts

Data items
Name, address, company, phone, position, DoB, email, purchase history, etc.

Trust boundaries (jurisdiction, geography)
Enterprise/legal entity
EU
Non-EU

Formats

Processing & transfer methods

Collect/create
Storage
Usage
Disclosure
Disposal

Data subject
Enterprise (internal)
3rd Parties
Data Flow Mapping - example

Collection/creation | Storage | Usage | Sharing/transfer | Disposal
---|---|---|---|---

DATA SUBJECT

Internet

"data minimisation"

Training Portal

"lawfulness, fairness & transparency"

EXTRENSE

Course Planner

"data minimisation"

Course execution

"accuracy" & "storage limitation"

THIRD PARTIES

Customer Campaigns

"purpose limitation"

B2B customers

Hosting firm

"accuracy" & "storage limitation"

Open waste containers

Data subject

"lawfulness, fairness & transparency"

Internet

"data minimisation"

Training Provider (F)

"integrity & confidentiality"

Data Analytics Firm

"purpose limitation"

Training Provider (F)

"lawfulness, fairness & transparency"

Hosting firm

"data minimisation"

Course Planner

"accuracy" & "storage limitation"

B2B customers

Training Provider (F)

"integrity & confidentiality"

Hosting firm

"data minimisation"

Course Planner

"accuracy" & "storage limitation"

B2B customers

Training Provider (F)

"integrity & confidentiality"

Hosting firm

"data minimisation"

Course Planner

"accuracy" & "storage limitation"

B2B customers

Training Provider (F)

"integrity & confidentiality"
## Data Flow Mapping - example

### Rights of the data subject
- Review privacy policies, privacy notices, employment contracts. Determine if special categories of personal data is involved and if children's data are involved.

### People & procedure risks
- Review/update contracts, data processor agreements, due diligence, etc.,

### Training course / xx / <company code & name> / Denmark / Group

<table>
<thead>
<tr>
<th>Collection/creation</th>
<th>Storage</th>
<th>Usage</th>
<th>Sharing/transfer</th>
<th>Disposal</th>
</tr>
</thead>
<tbody>
<tr>
<td>DATA SUBJECT</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Training Portal</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Extranet</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enterprise</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Customer Campaigns</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Third Parties</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>B2B customers</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hosting firm</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Analytics Firm</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Training Provider (F)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Rights of the data subject:
- Internet

### People & procedure risks:
- Open waste containers

### Review:
- Review privacy policies, privacy notices, employment contracts. Determine if special categories of personal data is involved and if children's data are involved.
Data flow elicitation techniques

Information about as-is data flows can be elicited using various techniques and combinations of them. Some people are more comfortable with one than another. Some like to share knowledge, others don’t. Some prefer to be visual, liner, physical etc.

Pros:
- Avoid time/effort documenting
- Reduce disturbing busy colleagues
- Useful if key resources are missing

Cons:
- May not exist
- May be out-to-date
- May not reflect what’s really happening

Inspect existing documentation

Pros:
- Consistent structure
- Can gather end-to-end input quickly if everyone’s available
- Teamthink – also good to reach consensus
- Saves time for the team in gathering individuals

Cons:
- Sometimes perceived as resource intensive
- Knowledge gaps if everyone is not available
- Extra effort in capturing information

Facilitated workshops with SMEs

Pros:
- Formal or informal
- Focused dialogue
- Builds relationships

Cons:
- Skill needed to capturing information
- Time consuming for the team
- Not good at reaching consensus about a data flow

Interviews with key resources

Pros:
- Elicit information from large groups of people
- Focused
- Easier analysis for closed questions

Cons:
- Analysis can be time consuming if questions are open-ended
- Not so good for building relationships

Questionnaires

Pros:
- Ability to spot good/bad habits or behaviour
- Can get clarification by asking immediately
- Good to spot environmental and behaviour aspects

Cons:
- Can be negatively disruptive
- Time consuming

Observation

Pros:
- Practical understanding and context
- Good to spot environmental aspects
- Builds relationships
- Sometimes easier to remember (physical experience)

Cons:
- Time consuming
- Extra effort in capturing information

Physical data flow walk through

=
Scope of this presentation

• The GDPR project – a new paradigm?
• Falck’s GDPR project – approach & structure
• Identifying GDPR project scope
• Identifying data flow scope
• Data flow mapping – an approach
• **Ensuring ongoing compliance**
• The human factor
• A slide for the busy executives
Context of the GDPR Project

Compliance Framework
(Data Protection Life-Cycle)

- Assess
  Risks/processes

- Protect
  Controls/Policies

- Respond
  Incidents/Breaches

- Sustain
  Compliance efforts
The project defines and implements a coherent set of policies, procedures, governance mechanisms and responsibilities to manage data protection and ensure ongoing compliance.
Compliance framework (tailored example)

### Policies
- Training & Awareness
- Data Protection Policy
- Trade Events
- Employee Data
- Mobile
- Telecommuting
- Social Media
- Compliance
- Privacy by Design

### Procedures
- Data Life Cycle Procedures
- Incident handling procedure
- Data Subject Requests procedures
- Breach notification procedure
- Monitoring & Reporting procedures
- Data Processor Agreement Procedure
- Data Protection Impact Assessment procedure

### Records
- Training records
- Data Subject Access Request Forms
- Data Processor Agreement Inventory
- Audit reports
- Consent Records Registry
- Data Protection Impact Assessment registry
- Privacy Notice Registry
- Data Inventory
- Breach registry
- Metrics
- Relevant Legislation Registry
- Risk Acceptance Database

### Additional Categories
- IT
- Information Security
- Risk Management

- Information Security Procedures
- IT Procedures
- Risk Procedures

GDPR Project to establish
Existing or others to establish
Compliance Framework

*Start from scratch or seek inspiration from elsewhere?*

Information Security Management System (ISMS)
e.g. ISO/IEC 27001:2013

Personal Information Management System (PIMS)
e.g. BS 10012:2017 (release date 3 April 2017)

Privacy Framework
ISO/IEC 29100:2011

NIST 800-53 Appendix J
Privacy Controls Catalog
Scope of this presentation

- The GDPR project – a new paradigm?
- Falck’s GDPR project – approach & structure
- Identifying GDPR project scope
- Identifying data flow scope
- Data flow mapping – an approach
- Ensuring ongoing compliance
- **The human factor**
- A slide for the busy executives
Your employees’ bad habits are your biggest cybersecurity risk.
The human factor - ABC

Awareness  Behaviour  Common sense
The human factor - ABC

**Awareness**
- **Think.**
- **Check.**
- **Share.**

**Behaviour**
- **All information you work with has value.**
- **All information you work with has value.**
- **All information you work with has value.**

**Common sense**
- **All information you work with has value.**
- **All information you work with has value.**
- **All information you work with has value.**
Scope of this presentation

- The GDPR project – a new paradigm?
- Falck’s GDPR project – approach & structure
- Identifying GDPR project scope
- Identifying data flow scope
- Data flow mapping – an approach
- Ensuring ongoing compliance
- The human factor
- **A slide for the busy executives**
Your Organisation’s GDPR Project Game Plan

Territorial scope
Global scope and includes processing activities by Your Organisation outside of the EU/EEA that target services to EU citizens, process EU citizen data (including employee data) or monitor data subjects’ behaviour within the EU.

Material scope
Personal data (any information relating to an identified or identifiable natural person) across the data life-cycle i.e. collected/created, stored, processed, shared and deleted.

Project organization
- **Project Sponsor**: Sally Sixpack
- **Steering Committee**:
  - Joe Soap
  - Jens Hansen
  - Sven Svensson
  - Mario Rossi
  - Jane Doe
- **Core project team**:
  - Compliance
  - Legal
  - Procurement
  - HR
  - IT
  - Information Security
- **External resources**:
  - GDPR project support/advisor
  - Legal support
  - Information Security support

Project scope

**Risks & Assumptions**

**Assumptions**
- Personal data in Your Organisation is primarily concentrated in HR systems and processes as well as CRM systems and processes
- Internal controls for data privacy can build upon the defined Information Security framework within Your Organisation
- Procedures and processes are not well defined in Your Organisation

**Risks**
- Understanding of assessment questionnaires require heavy legal assistance
- Not all personal data is identified

**Goal & objectives**
- **Financial**
  - Reduce the risk of financial loss and reputational damage resulting from penalties & claims
- **Customer**
  - Ability to demonstrate that Your Organisation’s business is compliant with the GDPR
  - Ability to demonstrate Your Organisation is in control of personal data
  - Ability to act on the enhanced data subject rights
- **Innovation**
  - Gain an overview of how and where personal data flows through Your Organisation’s business system
  - Gain an early view of data protection risks in new initiatives and projects

**Timeline**

<table>
<thead>
<tr>
<th>2017 Q1</th>
<th>Q2</th>
<th>Q3</th>
<th>Q4</th>
<th>2018 Q1</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Preparation</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Pilot</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Analysis assessment</td>
<td>Revise Privacy notices</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Revise agreements &amp; contracts</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Definition of Data Protection policies &amp; procedures</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Implementation of policies &amp; procedures</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Competency assessment</td>
<td>Training &amp; recruitment (int/ext)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Protection Awareness</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Gap &amp; risk Assessment</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identify gaps &amp; risks</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Plan remediation</td>
<td>Evaluate &amp; prioritise</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Control &amp; policy implementation</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Map critical data flows</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Set data flow scope</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mobilise the organization (resources, communications &amp; training)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Organizational Change Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Compliance Framework</strong> (Data Protection Life-Cycle)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assess Risks/processes</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Respond Incidents/Breaches</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Protect Controls/Policies</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sustain Compliance efforts</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Financial**
- Reduce the risk of financial loss and reputational damage resulting from penalties & claims
Thanks for your attention

Tim Clements CIPP/E, CIPM, CIPT, CRISC, CGEIT
GDPR Project Advisor / Project Manager / DPO Services
+45 6113 5106
tim@privacysquad.dk