

CLEMENS

GDPR COMPLIANCE

Copenhagen
August 17, 2017

GDPR – GENERAL DATA PROTECTION REGULATION

AGENDA

- **What's in it for me?**
- **The four phases of a GDPR compliance project**
 - Phase 1: Getting started and planning
 - Phase 2: Dataflow mapping and gap analysis
 - Phase 3: Implementation
 - Phase 4: Maintenance

WHAT'S IN IT FOR ME...?

- **Identifying and managing most significant risks for a reasonable investment**
 - ✓ Filling the *most important* gaps – the lions on the savanna
 - ✓ GDPR knowledge in the company
 - ✓ Mitigate risk of fines (up to 4 % of annual turnover) – or get fines in the lower end of the scale
 - ✓ Be ready to respond in case of an incident (contingency plans will be in place)
 - ✓ Mitigate risk of negative PR and brand damage
 - ✓ Lower risk of being strong-armed by unions or disgruntled customers

PHASE 1 – GETTING STARTED AND PLANNING!

- Secure support and pressure from top management
- Secure allocation of resources to project
- Choose a project manager and project team – and the right external counsel. Aim to do as much as possible yourself. Building up knowledge is crucial.
- Budget
- Realistic timeframe – be ambitious but don't overdo it.

PHASE 2 - DATA FLOW MAPPING AND GAP ANALYSIS

- **Data flow mapping**
 - The foundation for precautions against data breaches and responding to them efficiently
 - Identify key persons in each department of the company, who can point out where personal data is being processed.
 - Be honest!
 - External advisor should be able to provide tools enabling your company to conduct the data flow mapping with internal resources.
- **Gap analysis**
 - Identifying gaps and how to fill them
 - Legal support required
 - Solution description

PHASE 3 - IMPLEMENTATION

- **Filling the gaps according to gap analysis and key legal requirements for GDPR compliance, such as**
 - Adapting processes for processing of personal data – and write them down. *Accountability!*
 - Implement required adjustments to IT systems
 - Consider voluntary appointment of DPO
 - Training the organization in new policies and changing their mindset towards data protection
- Preparing required documentation and appropriate policies, among others
 - ✓ Record of processing activities – list of personal data processed by your company
 - ✓ Data processing agreements with data processors.

PHASE 3 - IMPLEMENTATION

- Preparing required documentation and appropriate policies, among others
 - ✓ Data protection policies
 - ✓ Cookie policy and privacy policy (for website)
 - ✓ Declaration of consent for employees
 - ✓ Declaration of consent for job candidates
 - ✓ Description of procedures for handling inquiries from individuals (data subjects)
 - ✓ Description of procedure for handling data leaks
 - ✓ PIA analysis (only required if high risk for data subjects)

PHASE 4 - MAINTENANCE

- Maintenance of documentation, e.g. in case of changes to data processing set up
- Stay updated on new legislation and guidelines
- Make a plan for conducting periodic audits
- Test processes and contingency plans

QUESTIONS!

CLEMENS