

2018-05.24

The data protection reform

The implementation within the Swedish Prison and Probation Service

Mats Olsson and Gustav Malis, The Swedish Prison and Probation Service

Mats Olsson

Head of informations security (CIO)
and DPO

The Swedish Prison and Probation
Service

Gustav Malis

Security consultant
Legal council

Secure State Cyber

Introduction

The data protection reform:

- A general data protection regulation [GDPR], (EU 2016/679)
- A data protection directive in the field of law enforcement (EU 2016/680)

The Swedish Prison and Probation Service, characteristics

- *Complex legislative landscape*
 - Multitude of legislations
 - Demarcation between different legislation
- *Substantial processing activities regarding personal data*
 - Many data subjects concerned by the processing
 - Large quantities of personal and sensitive personal data processed

Introduction

Initial pre-analysis by the DPO to estimate the overall consequences of the reform

- led to an activity list and special recommendations

Examples of new requirements in the data protection reform

- Obligation to communicate personal data breach
- Obligations relating to the concept of Privacy by design
- Increased requirements on the information to be given to the data subject
- Right of access: if the request is communicated through electronic means, the response has to be communicated in a commonly used electronic format
- DPO, increased mandates and responsibilities
- Increased administrative penalties

1. The GAP-analysis on the Swedish Prison and Probation service

2. The measures taken following the GAP-analysis

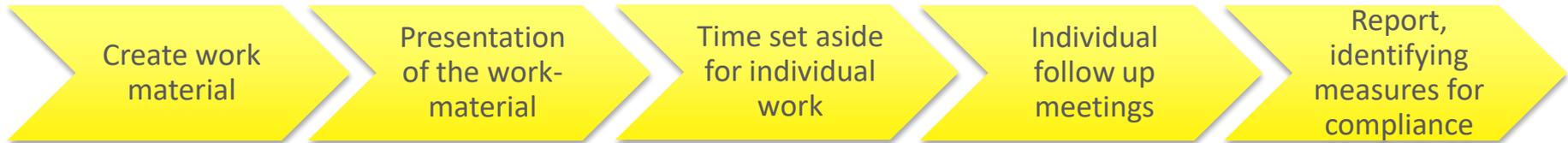
3. The continued work, challenges ahead

The GAP-analysis

- The GAP-analysis served a double purpose:
 - To identify measures that needed to be taken to further compliance with the EU data protection reform and,
 - To map the processing activities within the organisation and to properly document them
- A focus on the major information systems within the organisation (which manages large quantities of personal data or categories of sensitive personal data).
- Parallel to the information system analysis, an update and completion of the authority's official record of processing activities has been carried out

Method of the GAP-analysis

- A checklist based on the new rules in the EU data protection reform
- Support material with information explaining the context and purpose of the questions



Synergy effects of the analysis

- Mapping of the system-architecture
- Identification of the needs for system development
- Leverage for the overall work concerning information security
- Increased awareness of privacy and data protection issues within the organisation

2. The measures taken following the GAP-analysis

The measures taken

Two categories of measures were identified in the report of the GAP-analysis

- Measures relating to a specific information system
- Measures identifying an organisation wide need for action

Measures relating to a specific information system

Each branch of the organization, through their representatives, has been given the task to plan and carry out necessary measures in response to the identified measures in the GAP-analysis concerning their information systems and the to report back to the DPO for confirmation.

General measures taken

- The official record of processing
- Information to the data subjects
- Rules and procedures regarding e-mail and file storage
- Privacy by design measures (technical and organisational measures)
 - Procedures regarding DPIAs
- Review of the processing-agreements with processors
- Open text-fields
- General information measures to increase awareness within the organisation

3. The continued work and challenges ahead

Continued work.. discussion points

- DPO: nomination and organisational placement
- The limited retention principle, archiving and the erasure of data
- E-mail
- Right of access: response through electronic means if request by same means

Final questions or input?