Custodial Institutions Agency
Ministry of Justice and Security

Privacy @ Europris

Alexander Hoefmans
Gustav Malis
Bart Pieters

24 May 2018

PEBKAC

https://www.youtube.com/watch?v=yrjT8m0hcKU

Content

- Content:
  - Legal introduction: Alexander
  - Expected issues and overview approach: Bart
  - Swedish case study: Gustav
  - Case discussions
  - Wrap up
  - Q&A

- Questions: feel free to interrupt and/or at the end

Expected issues within prisons

Legitimacy

- Purpose limitation: data sharing across organisation borders
- Proportionality: collecting too much data
- Subsidiarity: unnecessarily invasive practices

People & behaviour

- Awareness during daily work, e.g. sharing data, new projectc
- Sufficiently skilled to deal with privacy issues
- Use of free services / Shadow IT: *'if the service is free, you are not the customer but the product being sold'*

Documentation

- Specific privacy documents: DPIA, Register (art. 30)
- Backlog/update
- Aimed at design: evidence is missing

Expected issues within prisons

IT

- Systems not designed to inform stakeholders
- Logging and monitoring
- Testing with anonymised/pseudonimised data
- Retention times

Procurement

- Update processing agreements for compliance
- Privacy requirements missing: purpose limitation, handling & protection including evidence, procedures for data breaches, retention, exit and migration, ownership of data

Transparancy/informing stakeholders

- Timely informing stakeholders across all systems
- Authentication of former employees or prisoners

A practical approach

General

- Work risk-based: start with the most sensitive data (health care)
- Don’t dash on a marathon, make small and constant improvements
- Privacy is never finished: it needs consistent attention
- Limit the level of detail: identify high level processes and use those: camera surveillance vs several sub processes and technical systems
- Add a touch of privacy to current projects
- Synchronised legitimacy with other laws

Governance

- Develop a compact privacy policy providing personnel with direction, e.g. ‘safety, security and health care take priority over privacy’
- Privacy-KPI in management control cycle
- Make it easy to manage: design a control plan tailored to the responsibilities of a prison director

A practical approach

Privacy support structure

- Appoint privacy officers throughout the organisation
- Make it easy to comply: develop/share guidelines, privacy-proof processes, templates, privacy courses

Privacy by design

- Embed privacy (and security) in all activities, documents and products: post-documenting & -corrections → it saves €€€ & 🕐
- Special attention for procurement, IT projects and research, HRM
- Begin with the end in mind (exit-strategy, retention times, deletion, migration to new services) and work your way back to procurement

Transparancy

- Take them to computer/file cabinet and show them
- Don’t mention the GDPR if they don’t
- Start with general answers

A practical approach

Personnel

- Provide guidelines and focus on ‘how to’
- Make it easy to comply: sufficient IT-services & ease of use
- Increase awareness and raise skill level:
  - Frequent short messages related to real world cases & relevant for their specific jobs
  - Train personnel: general and specific courses
  - Discuss privacy dilemma’s during regular team meetings

Privacy requirements

- Develop a privacy framework: privacy requirements → controls → underlying documents
- Document everything: privacy-analyses, designs, agreements, procedures, policies

Case 1

May I use real data of prisoners to evaluate operational policies and processes?

Answer 1

Yes, you may. Evaluating operational policies is simply part of the PDCA-cycle aimed at improving both policies and processes. Using data you collected for those processes is not a problem.

However, you must limit the privacy impact by:

- Limiting the data set: fields, subjects, time period
- Pseudonimisation of data: e.g. hashing of identifying data
- Anonymising the results: e.g. by aggregation
- Limiting and monitoring access to the real data
- Deleting the real data at a set point in time

Case 2

I want to share personal data with a professional partner. Processing by this partner is covered by law. May I share the information?

Answer 2

When sharing data across organisational borders, you need two-way legitimacy: both parties need to make sure they are allowed to send or receive the data.

In other words: you need to make sure you are allowed to share the information based on laws and regulations applicable to you, and your partner needs to do the same based on their legal framework to determine if they may receive the information.

Case 3

I want to email a dossier containing penal information to a different organisation within the justice departement. I am allowed to share this information, they are allowed to receive it. Is it ok to email it?

Answer 3

It depends on the level of security: within one department usually private networks are in place with sufficient security measures. In such a case emailing the dossier should be fine. Perform a risk analysis to be sure.

Case 4

On the network share, our team has many many thousands of files some of which contain personal data. It is impossible to sort through them all. Is that sufficient reason not to take action?

Answer 4

Unfortunately no! You should take steps to resolve this. It is possible to automatically clean house and remove files which have not been touched by an employee for x years. However take care to fulfil archiving compliance first.

Case 5

I want to set up a data warehouse, run big data analyses and correlate data from different sources. When I find exceptional results, I want to be able to drill down to the individual level, is that allowed?

Answer 5

It is not forbidden, however it is nearly impossible to do so and remain compliant. Basically with every correlation and report, you need to perform a privacy analysis to ensure legitimacy.

A better option is to pseudonimise and anonimise:

- Hash/encrypt/modify directly identifying information
- Aggregate detailed information in classes (e.g. age groups)
- Aggregate the results

→ Freedom to correlate and analyse

- Drill down to the individual → use the original data/system

Case 6

Auditors want to know when I'll be compliant with GDPR: how much time will it take to become compliant and how do I achieve this?

Answer 6

Privacy compliance is never finished: organisations, processes, people, laws etc. change all the time. Privacy has no finish line.

A good way to go is:

1. Current privacy improvement plans + progress reports
2. Governance: privacy embedded in management control cycle
3. Actual privacy by design

Case 7

I am a closing a contract to use software as a cloud service. The supplier a GDPR compliant and so is the agreement. Is that sufficient?

Answer 7

No, the supplier can at best guarantee data protection and provide services you can use to be compliant.

Things you have to do yourself:

- Ensure the contract has all the requirements *you* need
- Perform privacy analysis and ensure legitimacy
- Privacy implementation: retention period, autorisation rules, logging rules, organise for data breaches etc.
- Privacy proof use: current autorisations, monitor use, monitor data exports, report privacy incidents
- Clean exit: data return, data deletion (backups, logging) including evidence collection

Wrap up

If you forget everything else, please remember this:

1. Document and collect evidence
2. Work risk-based
3. Embed privacy by design
4. Embed privacy in the management control cycle and make small and constant improvements
5. Make sure people are aware and capable of dealing with privacy

Closing thoughts

https://www.youtube.com/watch?v=EjeZxySmYKA

Questions?