DNA3.1 - Report on the coordination of accounting data sharing amongst Infrastructures (initial phase)

Uros Stevanovic – NA3
NA3.2
KIT

AARC2 AHM, Athens
2018.04.11
DNA3.1 Deliverable

Initial phase

• “This document assess privacy regulations on accounting data needed by service operators and e/r-infrastructures to ensure smooth and secure service operations”

• Initial phase → “permission” to scope the doc

• “Secure operations” → risks?

• Timeline:
  • In the first phase → Risk assessment, DPIA
  • Second phase → doc expansion, more input

• Due date – end of April 2018

• Doc link:
  https://docs.google.com/document/d/19WJcYfESlHeiei10N4kyDApk1tosrLEDW49ERDapp4U/edit
Risk and risk assessment

- Risk – “scenario describing an event and its consequences, estimated in terms of severity and likelihood”
- Risk management – “coordinated activities to direct and control an organization with regard to risk”

- “Risks have to be identified, analyzed, estimated, evaluated, treated (e.g. mitigated...), and reviewed regularly.”
- Continuous assessment of risks
- Continuous mitigation of risks
GDPR Article 35(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.”
From WP29 – “Process to for building and demonstrating compliance” with the GDPR

Non-compliance may result in fines (2% or 10M€):
  • Failure
  • Wrong DPIA

European Data Protection Board (EDPB) and national DPA – guidelines, examples
  • Consistent GDPR application

Not mandatory
  • But as mentioned, continuous risk management is mandatory
High risk?  
Art 35(1,3,4)

Article 35:
1 – “Likely to result in high risks”
3 – “systematic and extensive evaluation, automatic processing, profiling, legal effects; large scale, special categories from Art 9(1); systematic monitoring of public area”
4 – DPA issued examples
DPIA decision schematic

High risk? Art 35(1,3,4)

- No
- Yes

Exceptions? Art 35(5,10)

- No DPIA necessary

Article 35:
- 5 – DPA issued exception examples
- 10 – DPIA already conducted as a part of a legal basis
DPIA decision schematic

High risk? Art 35(1,3,4)

Exception? Art 35(5,10)

No DPIA necessary

Article 35:
7 – Assessment description:
- Processing description
- Necessity and proportionality of the processing
- Risk assessment of the user’s rights
- Measures to mitigate risks, security measures for the protection of data, demonstrating GDPR compliance
DPIA decision schematic

High risk? Art 35(1,3,4)

- No
  - No DPIA necessary

- Yes
  - Exceptions? Art 35(5,10)
    - Yes
      - DPO, Compliance Art 35(2), 39(1c)
      - Article 35(2) – DPO input (if DPO exists)
      - Article 39(1c) – DPO should Monitor DPIA performance
    - No
      - DPIA Art 35(7)
DPIA decision schematic

High risk?
Art 35(1,3,4)

- No
- Yes

Exceptions?
Art 35(5,10)

- Yes
- No

DPO, Compliance
Art 35(2), 39(1c)

CoCo
Art 35(8)

Article 35(8) – Compliance with approved CoCo by the controllers

No DPIA necessary

DPIA
Art 35(7)
DPIA decision schematic

High risk? Art 35(1,3,4)

- No
  - No DPIA necessary
- Yes
  - Exceptions? Art 35(5,10)
    - No
      - DPIA Art 35(7)
    - Yes
      - DPO, Compliance Art 35(2), 39(1c)
        - No
          - CoCo Art 35(8)
        - Yes
          - Data subject’s view Art 35(9)

Article 35(9) – Seeking the view of data subjects, where appropriate
DPIA decision schematic

High risk? Art 35(1,3,4)

No

Yes

Exceptions? Art 35(5,10)

No DPIA necessary

DPO, Compliance Art 35(2), 39(1c)

CoCo Art 35(8)

Data subject’s view Art 35(9)

DPIA Art 35(7)

Controller’s review Art 35(11)

Article 35(11) – Controller conducts the review of processing to fit DPIA, especially when there is a change of risk
DPIA decision schematic

High risk? Art 35(1,3,4)

- No
  - No DPIA necessary
- Yes
  - Exceptions? Art 35(5,10)
    - Yes
      - DPO, Compliance Art 35(2), 39(1c)
      - CoCo Art 35(8)
      - Data subject’s view Art 35(9)
    - No
      - DPIA Art 35(7)

DPIA Art 35(7)

- Yes
  - Residual high risk? Art 36(1)
    - No
      - No prior consultation necessary
    - Yes
      - Prior consultation

- No
  - Controller’s review Art 35(11)
    - No
      - No prior consultation necessary
    - Yes
      - Prior consultation
When is DPIA necessary?

• One operation, or group of similar operations
• “Likely to result in high risks”, nine criteria
  • Evaluation or scoring
  • Automated decision making with legal or similar effects
  • Systematic monitoring
  • Sensitive data (or data of highly personal nature)
  • Data processing on a large scale
  • Matching or combining datasets
  • Innovative use or applying new technological or organizational solutions
  • Processing resulting in preventing data subjects from exercising a right or using a service or a contract
• Two or more → DPIA likely
• Sometimes even one is enough
How to conduct DPIA?

1. Description of the envisaged processing
2. Assessment of the necessity and proportionality
3. Measures already envisaged
4. Measures envisaged to address the risks
5. Assessment of the risks to the rights and freedoms
6. Monitoring and review
7. Documentation
### DPIA – risk table (CNIL)

<table>
<thead>
<tr>
<th>Risks</th>
<th>Impacts on data subjects</th>
<th>Main risk sources</th>
<th>Main threats</th>
<th>Existing or planned measures</th>
<th>Severity</th>
<th>Likelihood</th>
</tr>
</thead>
<tbody>
<tr>
<td>Illegitimate access to personal data</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unwanted change of data</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disappearance of data</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Privacy risks, security risks → can be considered together
Input from WISE risk management
## DPIA – risk of illegitimate access to data

<table>
<thead>
<tr>
<th>Risk</th>
<th>Main risk sources(^{56})</th>
<th>Main threats(^{57})</th>
<th>Main potential impacts(^{58})</th>
<th>Main controls reducing the severity and likelihood(^{59})</th>
<th>Severity(^{60})</th>
<th>Likelihood(^{61})</th>
</tr>
</thead>
<tbody>
<tr>
<td>Illegitimate access to personal data</td>
<td>Rogue acquaintances</td>
<td>Data theft/consultation on the server</td>
<td>Consequences of the disclosure of potentially sensitive information (discrimination, threats, attacks, loss of employment, loss of access to services, etc.) Phishing Targeted advertising</td>
<td>Minimization Storage durations Logical access control Stream encryption (SSL) Hardware authentication Private cloud Logical access control Employee clearance Access logging Log audits Notification of data subject violations and recommendation of suitable preventive controls</td>
<td>Significant</td>
<td>Maximum</td>
</tr>
</tbody>
</table>
## DPIA – risk of unwanted change of data

<table>
<thead>
<tr>
<th>Risks</th>
<th>Main risk sources</th>
<th>Main threats</th>
<th>Main potential impacts</th>
<th>Main controls reducing the severity and likelihood</th>
<th>Severity</th>
<th>Likelihood</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unwanted change of data</td>
<td>Negligent or rogue user/family member/friend</td>
<td>Alteration of data on the server</td>
<td>Identity theft</td>
<td>Backup of the cloud server</td>
<td>Limited</td>
<td>Limited</td>
</tr>
<tr>
<td></td>
<td>Rogue neighbor</td>
<td></td>
<td>Deterioration in the service quality</td>
<td>Stream encryption (SSL)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Negligent or rogue employee</td>
<td></td>
<td></td>
<td>Hardware authentication</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Hacker targeting one of the companies</td>
<td></td>
<td></td>
<td>Private cloud</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Logical access control</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Employee clearance</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Access logging</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Log audits</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Notification of data subject violations and recommendation of suitable preventive controls</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# DPIA – risk of data disappearance

<table>
<thead>
<tr>
<th>Risks</th>
<th>Main risk sources</th>
<th>Main threats</th>
<th>Main potential impacts</th>
<th>Main controls reducing the severity and likelihood</th>
<th>Severity</th>
<th>Likelihood</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disappearance of data</td>
<td>Negligent or rogue user/family member/friend</td>
<td>Erasure of data (via the app or server) Deterioration of servers Physical damage to the device</td>
<td>Need to recreate a user account Loss of history and personal service settings Deterioration in the service quality</td>
<td>Backup of the cloud server Private cloud Physical protection of the cloud servers Maintenance Temporary on-premises data retention Logical access control Employee clearance Strong authentication of employees Access logging Warranty for the device</td>
<td>Limited</td>
<td>Limited</td>
</tr>
</tbody>
</table>
GIODO (The Inspector General for the Protection of Personal Data) opinion (Polish DPA)

<table>
<thead>
<tr>
<th>Types / criteria for processing operations for which assessment is required</th>
<th>Examples of operations / data scope / circumstances in which a high risk of a breach may occur for a given type of processing operation</th>
<th>Potential areas of occurrence / existing areas of application</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cross-border data processing</td>
<td>Processing data of students, trainees and transmission outside academic staff by universities, as part of the European Union exchange and research programs, which is not covered by agreements between the Republic of Poland and third countries (e.g. data on students participating in exchanges between universities)</td>
<td>Universities participating in international scientific programs</td>
</tr>
<tr>
<td></td>
<td>Processing of HR data in international corporations established outside the EU</td>
<td>Keeping central HR documentation</td>
</tr>
<tr>
<td></td>
<td>Data processing using public cloud computing resources located in third countries</td>
<td>Use of cloud services provided by international corporations</td>
</tr>
</tbody>
</table>
DPIA – research communities

• IdP-SP (or AA) scenario

• Three “sources” of personal information:
  • Information provided by the users (release of information from the IdP)
  • Information provided about the user by external party (information contained in the IdP-proxy, e.g. group management, unique identifiers, etc.)
  • Information containing users’ personal info created by other processing activities (logging, accounting, monitoring)

• Information:
  • Email and user’s actual name (usernames)
  • Usage of resources (e.g.)
  • Medical data, special personal data (sensitive, not extensively considered at the moment)
Summary

• DPIA, or at the very least risk assessment process has to be conducted
• Continuous process
• Documentation!
• Process:
  • Description of data processing
  • Necessity and proportionality
  • Identifying and assessing risks
  • Measures to mitigate risks
  • Record outcomes
  • Integrate outcomes into actionable plan
  • Review (reiterate)
AND NOW FOR SOMETHING COMPLETELY DIFFERENT.
DNA3.1

• “Report on the coordination of accounting data sharing amongst Infrastructures”
• Accounting data use-cases? ➔ Feedback/info needed!
Thank you
Any Questions?

uros.stevanovic@kit.edu
References

- Andrew Cormack’s presentations (and talks, posts..)
- DNA3.1 Google doc - https://docs.google.com/document/d/19WJcYfESlHeiei10N4kyDApk1tosrLEDW49ERDapp4U/edit