Authentication and Authorisation for Research and Collaboration

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

Risk assessment and Data Protection Impact Assessment (DPIA)

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.”

DPIA

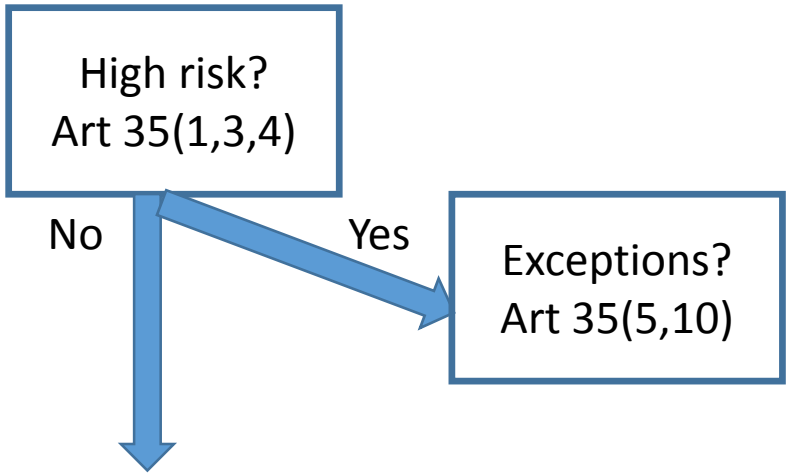
- From WP29 – “Process to for building and demonstrating compliance” with the GDPR
- Non-compliance may result in fines (2% or 10M€):
  - Failure
  - Wrong DPIA
- European Data Protection Board (EDPB) and national DPA – guidelines, examples
  - Consistent GDPR application
- Not mandatory
  - But as mentioned, continuous risk management is mandatory

DPIA decision schematic

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

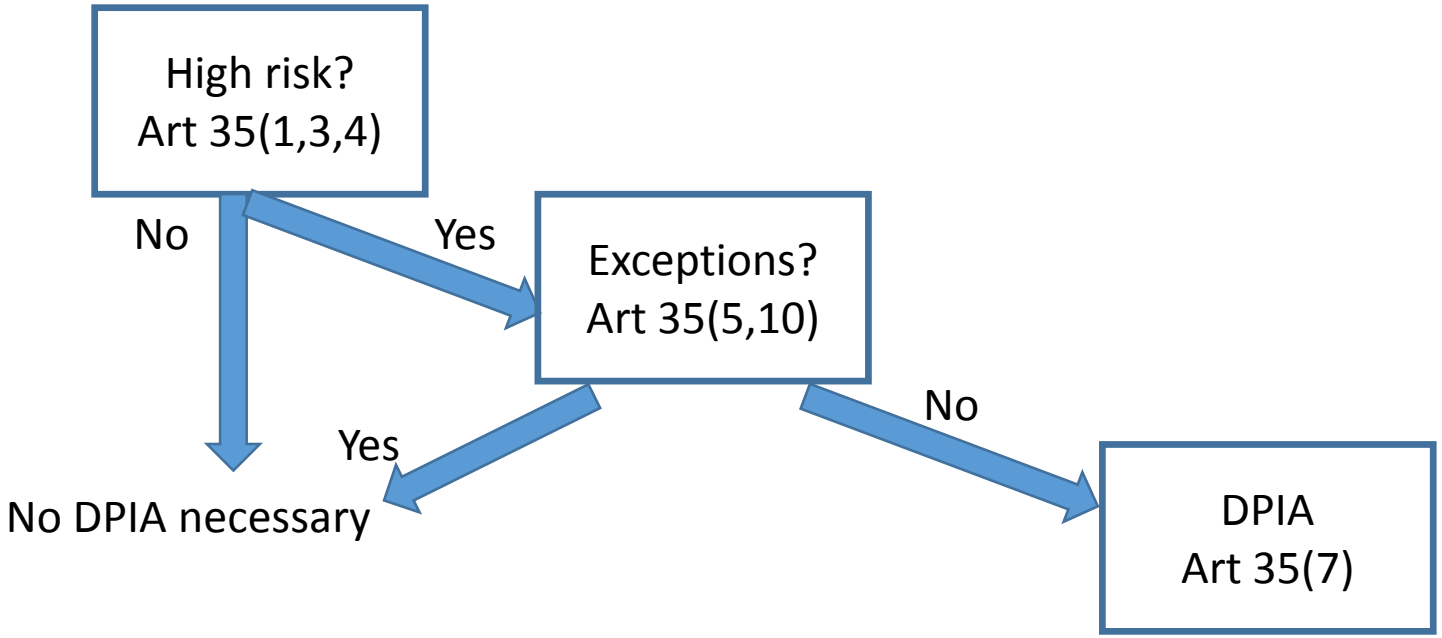
Article 35:
1 – “Likely to result in high risks”
3 – “systematic and extensive evaluation, automatic processing, profiling, legal effects; large scale, special categories from Art 9(1); systematic monitoring of public area”
4 – DPA issued examples

DPIA decision schematic



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

DPIA decision schematic

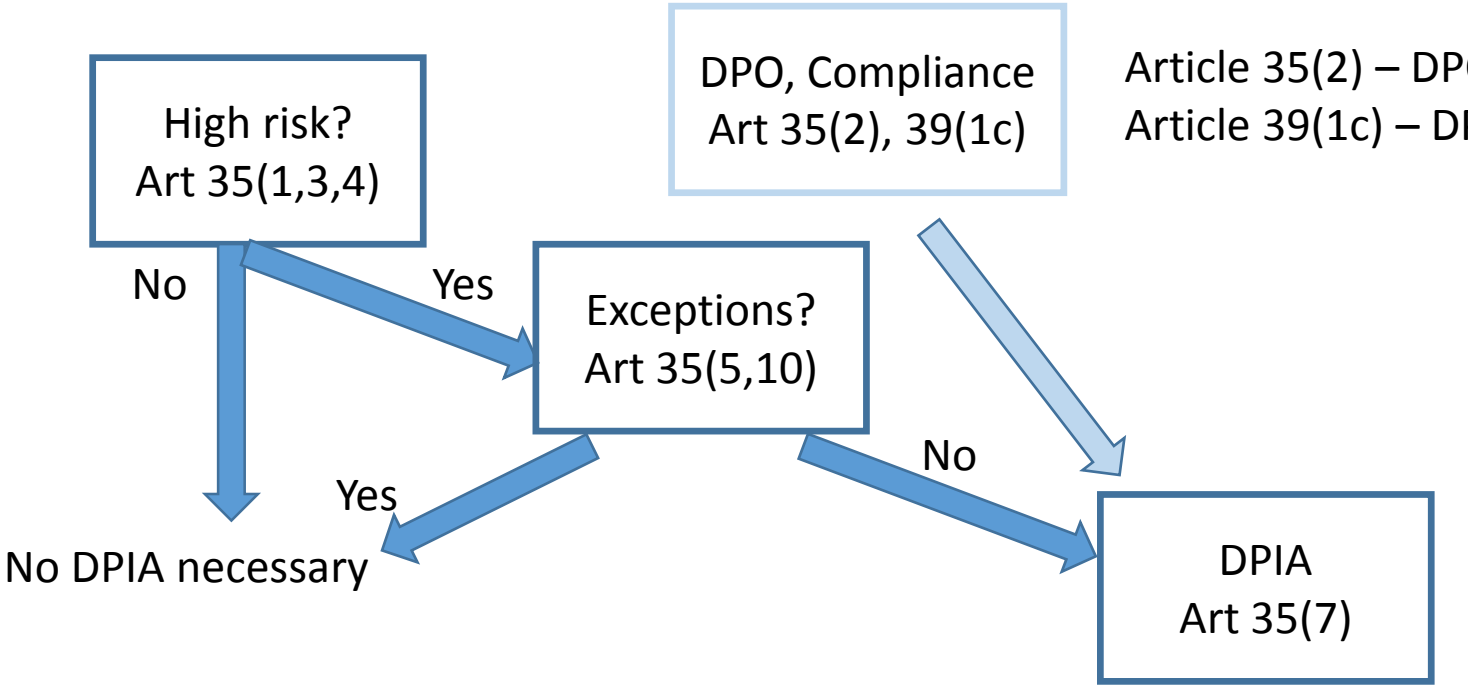


Article 35:

7 – Assessment description:

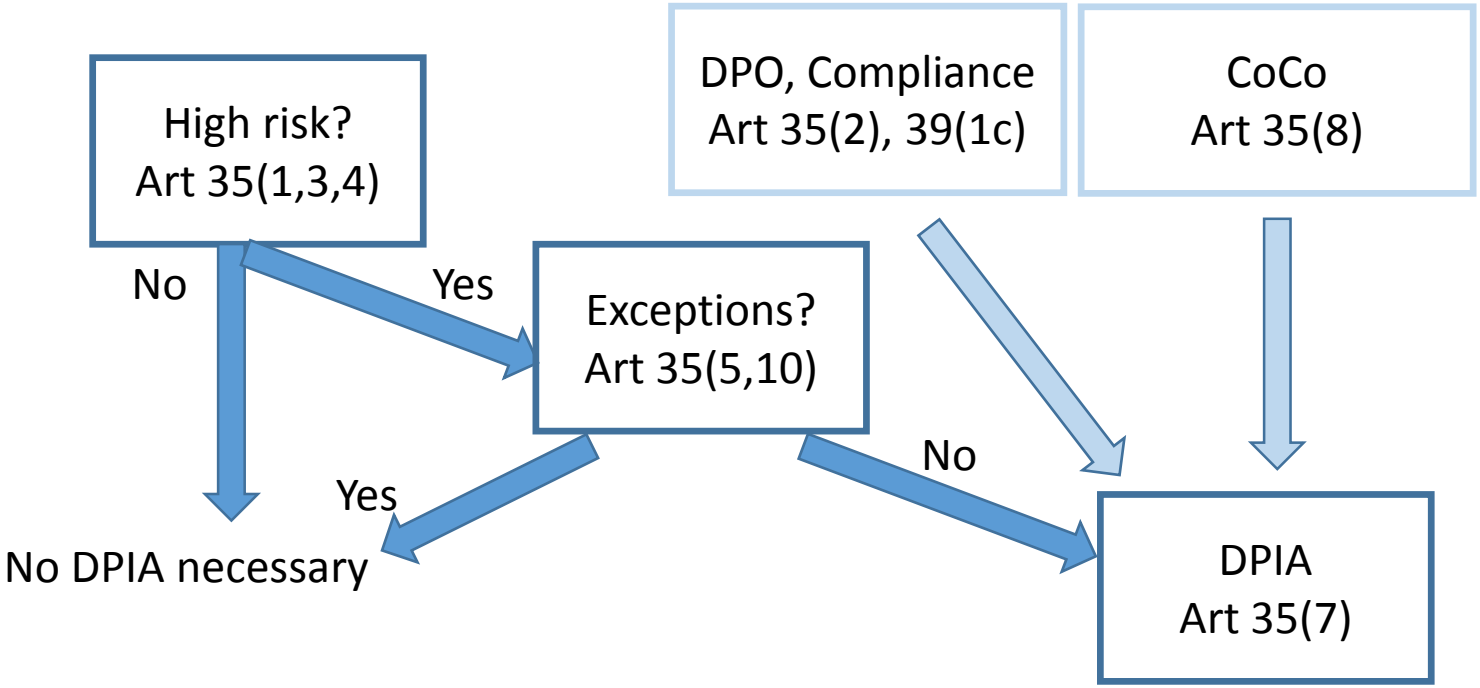
- Processing description
- Necessity and proportionality of the processing
- Risk assessment of the user's rights
- Measures to mitigate risks, security measures for the protection of data, demonstrating GDPR compliance

DPIA decision schematic



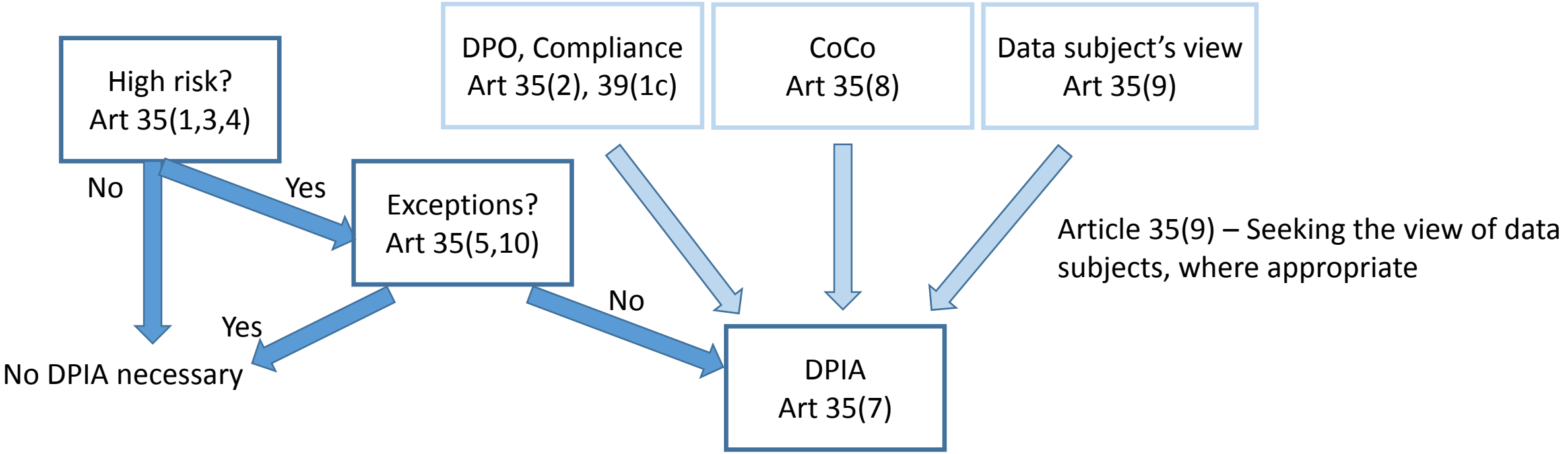
Article 35(2) – DPO input (if DPO exists)
Article 39(1c) – DPO should Monitor DPIA performance

DPIA decision schematic



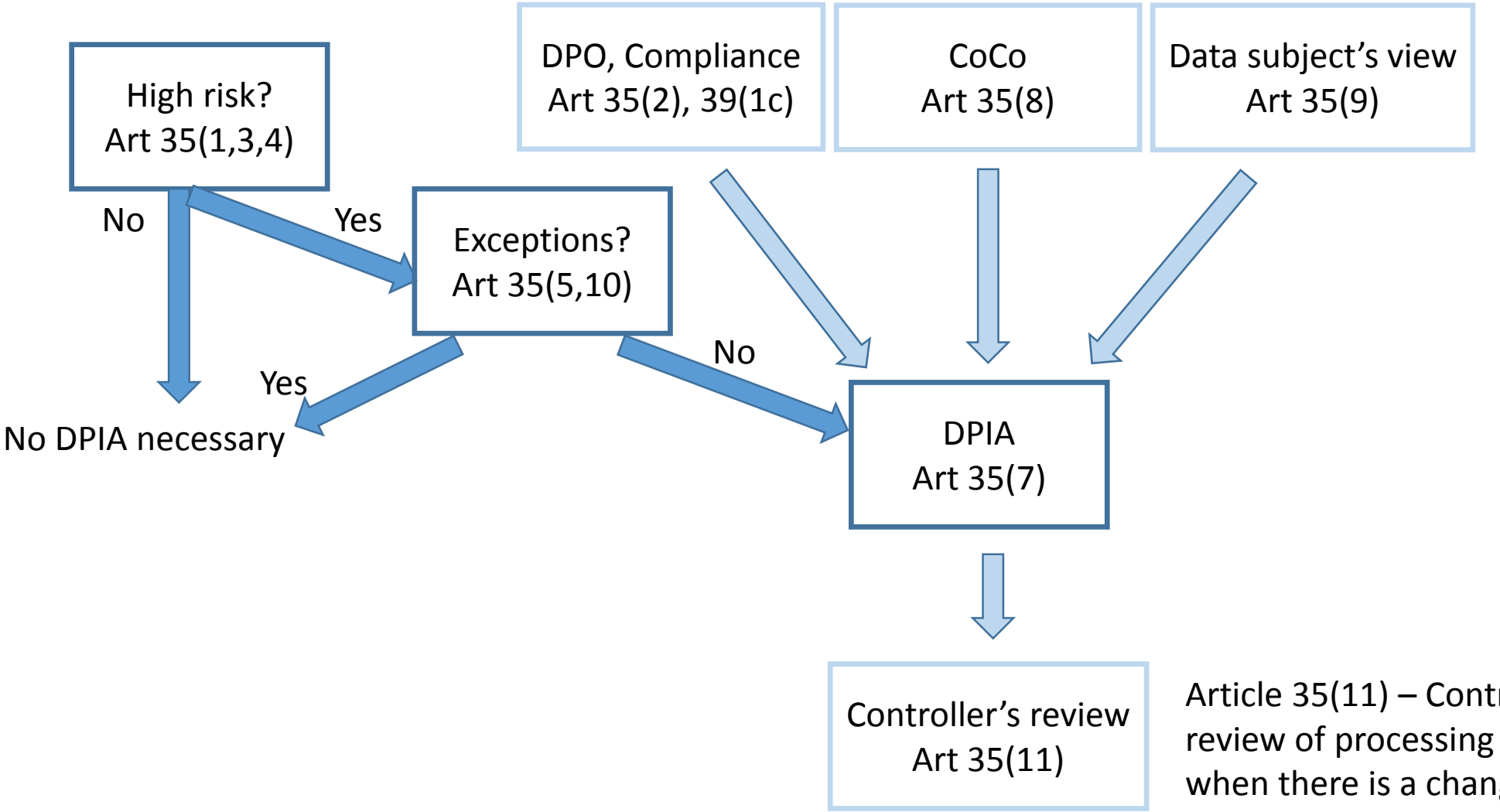
Article 35(8) – Compliance with approved CoCo by the controllers

DPIA decision schematic



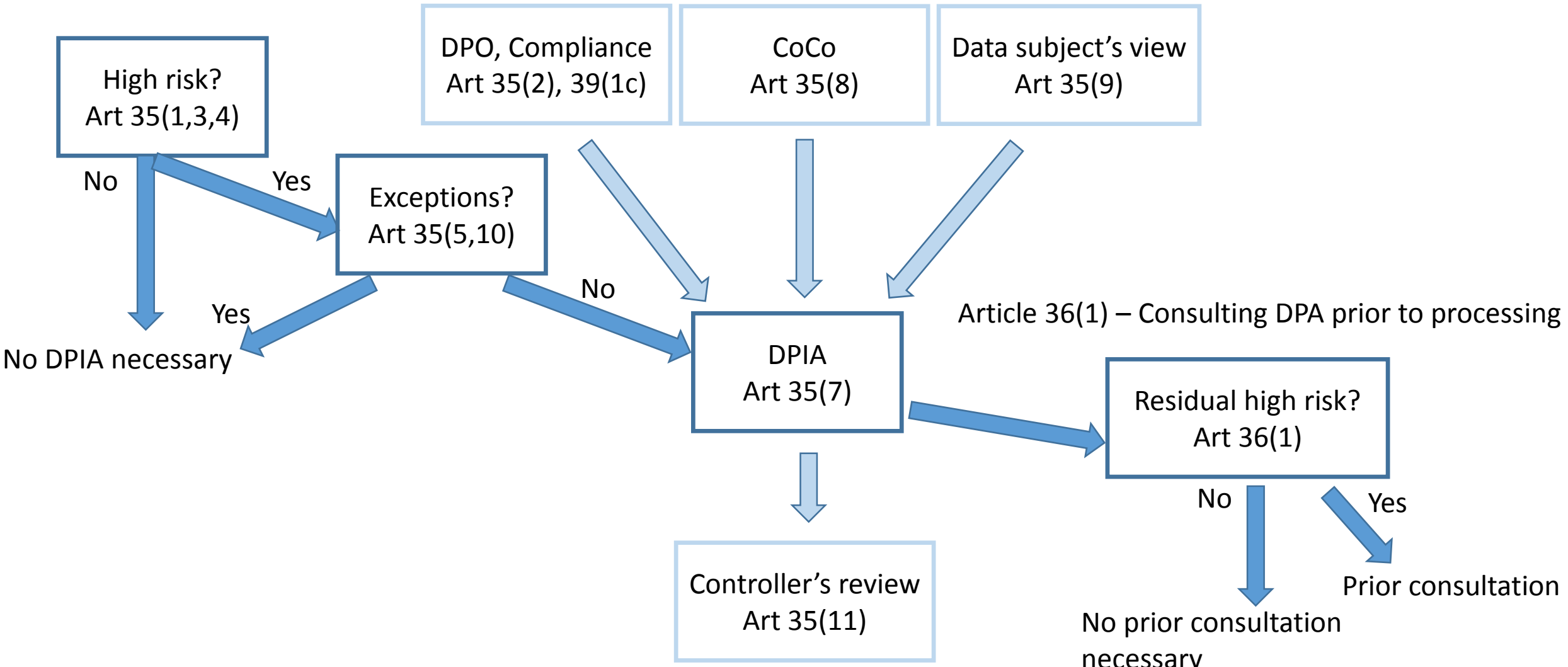
Article 35(9) – Seeking the view of data subjects, where appropriate

DPIA decision schematic



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

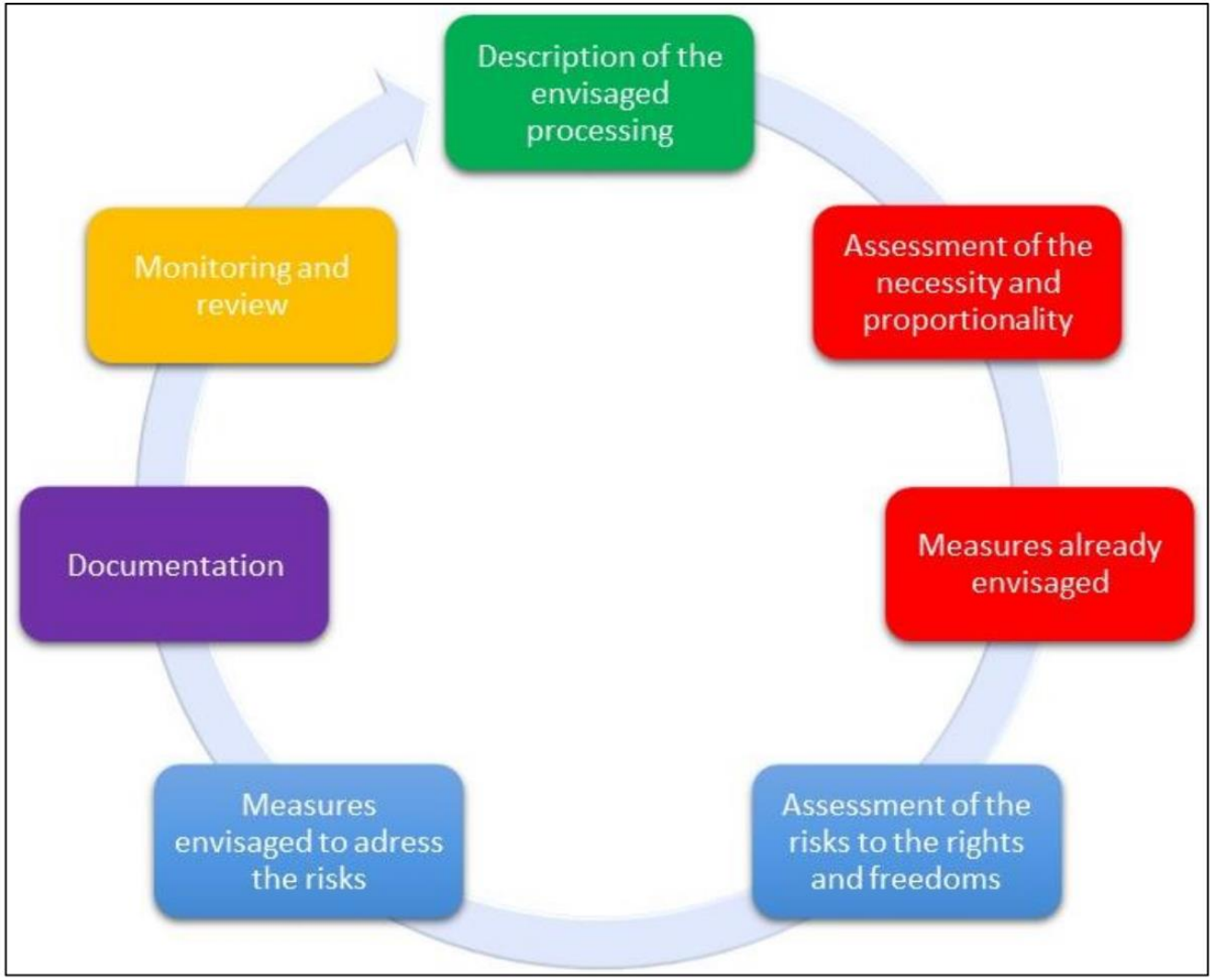
DPIA decision schematic



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?



DPIA – risk table (CNIL)

Risks	Impacts on data subjects	Main risk sources	Main threats	Existing or planned measures	Severity	Likelihood
Illegitimate access to personal data						
Unwanted change of data						
Disappearance of data						

Privacy risks, security risks → can be considered together
Input from WISE risk management

DPIA – risk of illegitimate access to data

Risk	Main risk sources[56]	Main threats[57]	Main potential impacts[58]	Main controls reducing the severity and likelihood[59]	Severity[60]	Likelihood[61]
Illegitimate access to personal data	Rogue acquaintances Rogue neighbor Rogue employee Authorized third-party company Hacker targeting a user or one of the companies	Data theft/consultation on the server Account theft (via a smartphone) Recovery of a scrapped device	Consequences of the disclosure of potentially sensitive information (discrimination, threats, attacks, loss of employment, loss of access to services, *etc.*) Phishing Targeted advertising	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	Significant	Maximum

DPIA – risk of unwanted change of data

Risks	Main risk sources	Main threats	Main potential impacts	Main controls reducing the severity and likelihood	Severity	Likelihood
Unwanted change of data	Negligent or rogue user /family member /friend Rogue neighbor Negligent or rogue employee Hacker targeting one of the companies	Alteration of data on the server	Identity theft Deterioration in the service quality	Backup of the cloud server 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	Limited	Limited

DPIA – risk of data disappearance

Risks	Main risk sources	Main threats	Main potential impacts	Main controls reducing the severity and likelihood	Severity	Likelihood
Disappearance of data	Negligent or rogue user /family member /friend Negligent or rogue employee Hacker targeting a user or one of the companies Damage at one of the companies	Erasure of data (via the app or server) Deterioration of servers Physical damage to the device	Need to recreate a user account Loss of history and personal service settings Deterioration in the service quality	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	Limited	Limited

GIODO (The Inspector General for the Protection of Personal Data) opinion (Polish DPA)

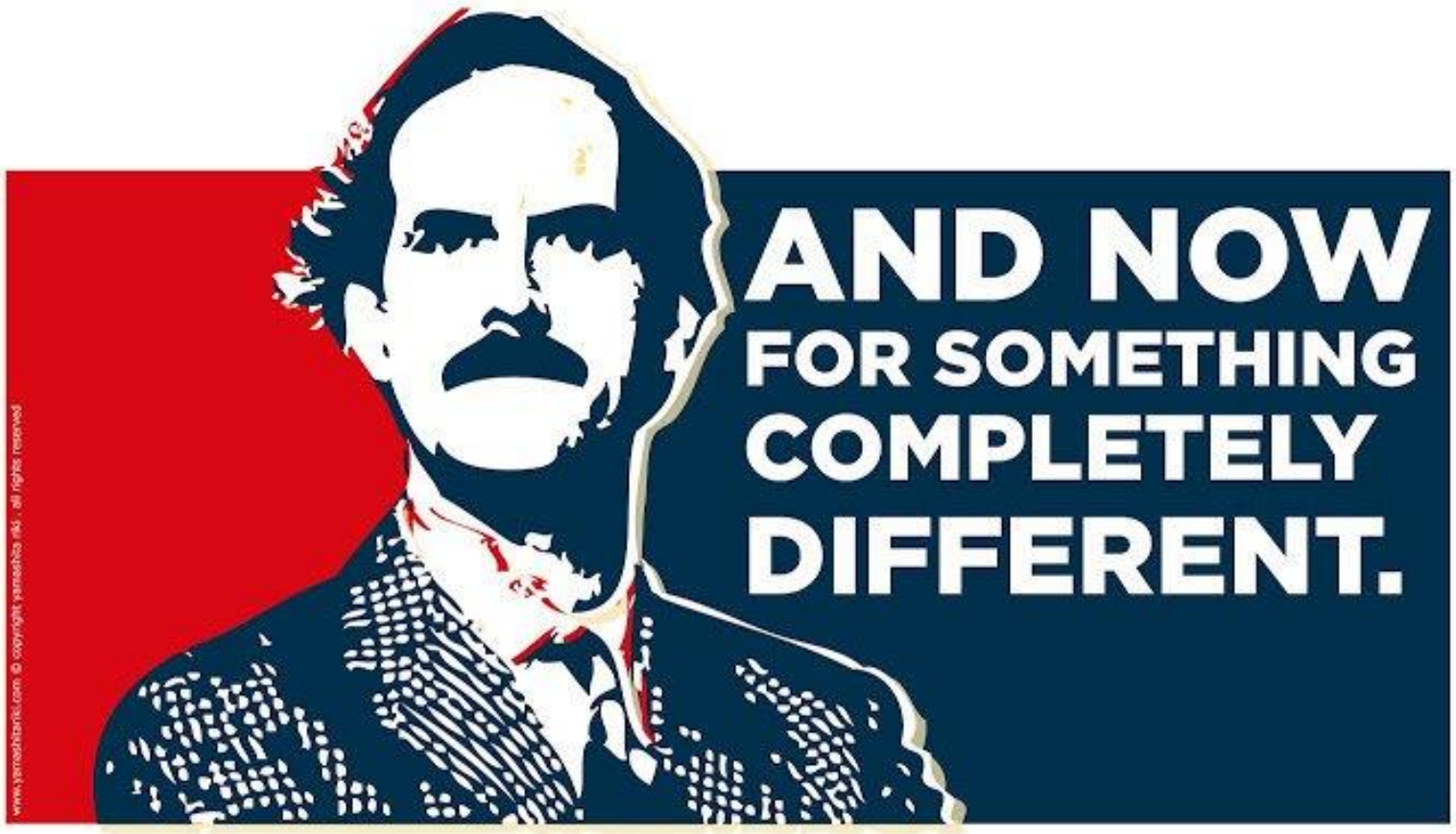
Types / criteria for processing operations for which assessment is required	Examples of operations / data scope / circumstances in which a high risk of a breach may occur for a given type of processing operation	Potential areas of occurrence / existing areas of application
Cross-border data Processing data of students, trainees and transmission outside academic staff by universities, as part of the European Union	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)	Universities participating in international scientific programs
	Processing of HR data in international corporations established outside the EU	Keeping central HR documentation
	Data processing using public cloud computing resources located in third countries	Use of cloud services provided by international corporations

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

https://aarc-project.eu

The work leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 730941 (AARC2).

References

- https://www.cnil.fr/en/cnil-publishes-update-its-pia-guides
- https://ec.europa.eu/newsroom/document.cfm?doc_id=47711
- https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/data-protection-impact-assessments-dpias-guidance/
- Andrew Cormack's presentations (and talks, posts..)
- https://wise-community.org/risk-assessment-template/
- DNA3.1 Google doc - https://docs.google.com/document/d/19WJcYfESlHeiei10N4kyDApk1tosrLEDW49ERDapp4U/edit