# PERSONA impact assessment training (IV): practical exercise

**Alessandra CALVI, Simone CASIRAGHI, Nikolaos IOANNIDIS, AND Dariusz KLOZA**

**Vrije Universiteit Brussel (VUB)**
Research Group on Law, Science, Technology & Society (LSTS)
Brussels Laboratory for Data Protection & Privacy Impact Assessments (d.pia.lab)

**27 May 2020**
*online*

VRIJE UNIVERSITEIT BRUSSEL

LSTS
LAW, SCIENCE, TECHNOLOGY & SOCIETY STUDIES
VRIJE UNIVERSITEIT BRUSSEL

# Agenda

*Quiz*

1. Recast
   - the framework
   - the method
2. Introduction to the case study
3. Group exercise
4. Next steps in the PERSONA project
5. Q&A

# The framework

1. systematic process
2. considers the relevant societal concerns
3. not everything needs it
4. uses the appropriate method
5. includes recommendations
6. a best efforts obligation
7. relies on sufficient knowledge and know-how
8. documented & transparent
9. deliberative
10. accountable
11. assessor is independent
12. simple
13. adaptive
14. inclusive
15. receptive
16. grows in supportive environment


d.pia.lab

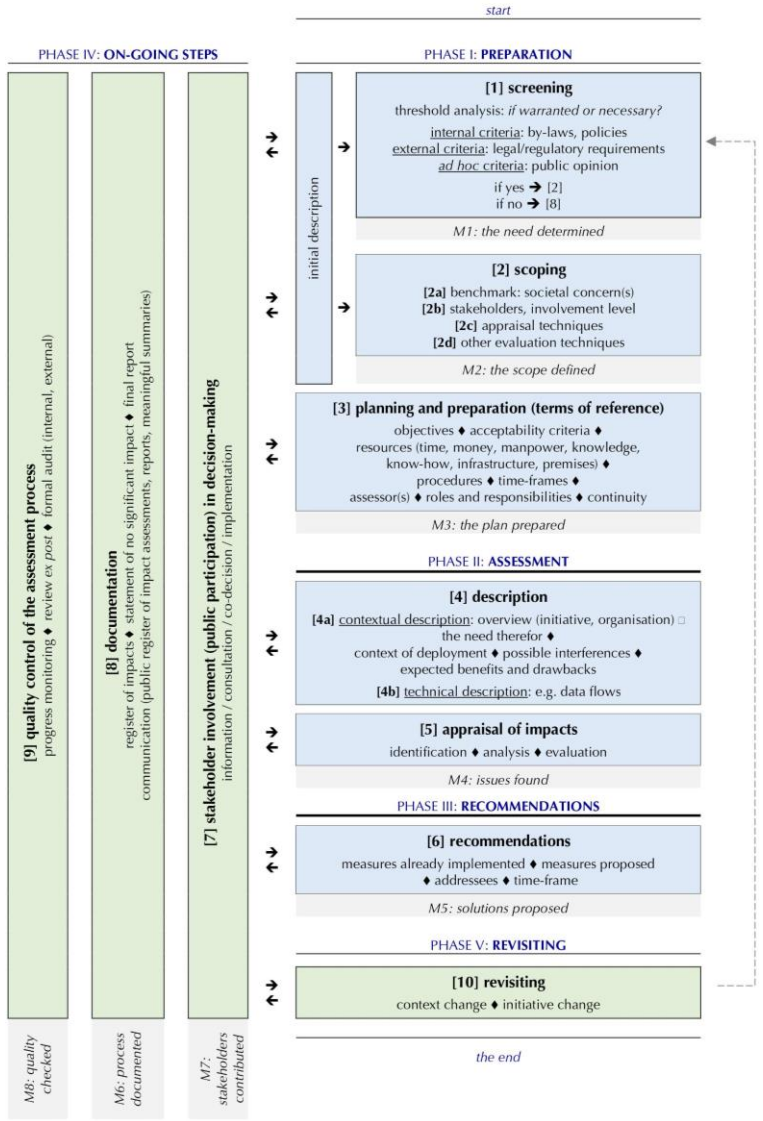
Data protection impact assessments in the European Union: complementing the new legal framework towards a more robust protection of individuals

d.pia.lab Policy Brief No. 1/2017

VRIJE UNIVERSITEIT BRUSSEL

LSTS LAW, SCIENCE, TECHNOLOGY & SOCIETY STUDIES VRIJE UNIVERSITEIT BRUSSEL

# The method




Source: Dariusz Kloza, *The concept of impact assessment in European privacy and personal data protection law*, Brussels, 2019

VRIJE UNIVERSITEIT BRUSSEL

LSTS
LAW, SCIENCE, TECHNOLOGY & SOCIETY STUDIES
VRIJE UNIVERSITEIT BRUSSEL

# Case study

## iBorderCtrl project (2016-2019)

- European Commission's **Research Programme "Secure Societies – protecting freedom and security of Europe and its citizens"**

- **The aim of iBorderCtrl** was to enable faster and thorough border control for third country nationals crossing the land borders of EU Member States:

- 2 Stages identification process
  1. Pre-screening
  2. At the actual border

# Critiques to iBorderCtrl project

- **The press**: critique of “Automated Deception Detection System” technology (e.g. The Guardian)

- **Civil society**: risk of discrimination, fundamental rights infringements (e.g. Homo Digitalis)

# An example

| | | | |
|---|---|---|---|
| 3 | Unlawful collection and storage of sensitive/ classified/special categories of data | *a. Option to delete historical diagnostic data by Device ID* | Consider deleting some specific users and creating new accounts for them |
| | | *b. Guarantee never to store content data in telemetry data or in other system-generated event logs unless strictly necessary* | Prohibit users from sending personal data to Microsoft to 'improve' Office |
| | | | Consider pilot with other software for some functionality (after conducting a separate DPIA) |
| 4 | Incorrect qualification Microsoft as data processor | *a. Minimisation of purposes to be able to act as a processor OR New framework agreement as joint controller* | Endorse new framework agreement as processor or joint controller |
| | | *b. Only process data from voluntary Connected Services as a data processor OR change default for voluntary Connected Services to 'Off'* | Prohibit voluntary Connected Services unless Microsoft offers these services as a processor |
| 5 | Not enough control over sub-processors and factual processing | *More audit rights* | Consider stand-alone deployment without Microsoft account for confidential/sensitive data |
| 6 | The lack of purpose limitation | *Processing only for strictly necessary purposes for which the tenants have a legal ground* | - no specific measure, see above |
| 7 | The transfer of data outside of the EEA | *New contractual guarantees and/or storage of diagnostic data within the EU* | - no specific measure, see above |
| 8 | The indefinite retention period of diagnostic data | *Determine necessary retention periods* | - no specific measure, see above |

## What can the admins do now to lower the risks?

Admins of the Enterprise version of Office ProPlus can already take a number of specific measures to lower the privacy risks for employees and other people in the Netherlands.

- Apply the new zero-exhaust settings
- Centrally prohibit the use of Connected Services
- Centrally prohibit the option for users to send personal data to Microsoft to 'improve Office'
- Do not use SharePoint Oneline / OneDrive
- Do not use the web-only version of Office 365
- Periodically delete the Active Directory account of some VIP users, and create new accounts for them, to ensure that Microsoft deletes the historical diagnostic data
- Consider using a stand-alone deployment without Microsoft account for confidential/sensitive data
- Consider conducting a pilot with alternative software, after having conducted a DPIA on that specific processing This could be a pilot with alternative open source productivity software. This would be in line with the Dutch government policy to promote open standards and open source software.

These measure are not in all cases realistic or feasible. It is not possible for the (Enterprise) customers of Office to solve all problems. With regard to the contracts and transfer of personal data to the USA, a European solution must be sought.

PRIVACY COMPANY

VUB VRIJE UNIVERSITEIT BRUSSEL

LSTS LAW, SCIENCE, TECHNOLOGY & SOCIETY STUDIES VRIJE UNIVERSITEIT BRUSSEL

# Practical exercise

1. Why (not) to do a DPIA?
   Why (not) to do other types of impact assessments?
2. How would you define the benchmark for the impact assessment process?
3. What type of expertise should be included in the team of assessors?
4. What types of (personal) data are to be processed?
5. What types of privacy are affected?
6. What are the possible impacts on fundamental rights beyond privacy and data protection?
7. What types of ethical concerns the technologies raise?
8. What could be the issues related to social acceptance of these technologies?
9. Are the technologies necessary?
   Are they proportionate?
10. What are the risks?
    How do you assess them?
11. Who, if ever, is to be consulted?
12. What are the possible mitigation measures?
13. When would you revisit the impact assessment?
    Why?
14. How do you document your process?
15. Who is going to check the quality of the process?
    How?
16. ...

# Thank you!

alessandra.calvi@vub.be
simone.casiraghi@vub.be
nikolaos.ioannidis@vub.be
dariusz.kloza@vub.be

LSTS.research.vub.be
dpialab.org
@dpialab

PERSONA
Co-funded by the Horizon 2020
Framework Programme of the European Union

VRIJE UNIVERSITEIT BRUSSEL

LSTS
LAW, SCIENCE, TECHNOLOGY & SOCIETY STUDIES
VRIJE UNIVERSITEIT BRUSSEL