how to do a data protection impact assessment?

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)

Brussels, 26 June 2019
Brussels Privacy Hub
4th European Data Protection Law Summer School
Advancing (with) EU data protection
all about us

- the **Research Group on Law, Science, Technology & Society** (LSTS) at Vrije Universiteit Brussel (VUB), created in 2003
- works predominantly in English
- ca. 50 full-time researchers
- 3 spin-off’s:
  - Brussels Privacy Hub
  - Privacy Salon
  - Brussels Laboratory for Data Protection & Privacy Impact Assessments (**d.pia.lab**), created in 2015
- 1\textsuperscript{st} policy brief of **d.pia.lab** (framework) published in May 2017 [EN] [FR]
- 2\textsuperscript{nd} policy brief of **d.pia.lab** (method) expected in June 2019 [EN] [FR]
An impact assessment is a tool used for the analysis of possible consequences of an initiative on a relevant societal concern or concerns, if this initiative can present dangers to these concerns, with a view to support the informed decision-making whether to deploy this initiative and under what conditions, ultimately constituting a means to protect these concerns.

(Kloza et al. 2017: 1)
supporting the conduct of D/PIA

- frameworks, handbooks, guidelines, manuals, ...
- templates, questionnaires
- awareness-raising, education, training, ...
- academic & professional literature, policy documents, ...
- bilaterals, word-of-mouth
- advice & feedback from DPAs (‘reference centres’)
- software for the automation of D/PIA
- ...

VUB LSTS LAW, SCIENCE, TECHNOLOGY & SOCIETY RESEARCH GROUP
a (subjective) ideal D/PIA

1. Systematic process
2. Considers the relevant societal concerns
3. Not everything needs it
4. Uses the appropriate method
5. Includes recommendations
6. Constitutes best efforts obligations
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
by what means? METHOD

Phase I: Preparation
1. Screening
2. Scoping
3. Planning

Phase II: Assessment
4. Description
5. Appraisal (identification, analysis and evaluation)

Phase III: Recommendations
6. Recommendations

(On-going phase)
7. Documentation
8. Stakeholder (public) involvement
9. Quality control

Revisiting
10. Revisiting
what?

- 1995 Art 20 Directive 95/46 (prior checking)
- 2009 RFID
- 2012 smart grids
- 2016 Arts 35-36 GDPR
- 2016 Art 27 Directive 2016/680
- 2018 Arts 39-40 & Art 42 Regulation 2018/1725
- 2019 Art 6 ePrivacy Regulation (proposal)
- 2019 Recital 53 re-use PSI Directive (proposal)
- ...

Article 35

**Data protection impact assessment**

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 operations that present similar high risks.

2. The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.

3. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:

   (a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

   (b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or

   (c) a systematic monitoring of a publicly accessible area on a large scale.
by what means?

1. **threshold**
   - criterion 1: *high risk* YES
   - criterion 2: *specific cases (3)* YES
   - criterion 3: *(national) exclusion list* NO
   - criterion 4: *(national) inclusion list* YES
   - criterion 5: *already carried out* NO
   - criterion 6: *professionals* NO

2. **description**
   - technical
   - contextual

3. **appraisal**
   - necessity & proportionality
   - risks to the rights & freedoms of individuals (all relevant human rights)

4. **stakeholder involvement**
   - when appropriate, data subjects or their representatives
   - due respect for legitimate secrecy
   - if appointed, consultation with a data protection officer

5. **recommendations: measures envisaged to:**
   - address the risks
   - ensure compliance with the GDPR

6. **prior consultation**
   - high residual risk
   - possible ban of processing

7. **re-visiting**
   - when necessary
practical exercise

1. why (not) to do a DPIA?
2. what (personal) data are to be processed?
3. is it necessary? is it proportionate?
4. what are the risks? how do you assess them?
5. who, if ever, is to be consulted?
6. what are the mitigation measures?
7. will you re-visit your DPIA? when?
8. ...
dank u!

dariusz.kloza@vub.be

@darekkloza

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