towards a method for data protection impact assessment: making sense of GDPR requirements

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)

Salzburg, 28 February 2020
Universität Salzburg
Internationales Rechtsinformatik Symposium IRIS 2020:
Verantwortungsbewusste Digitalisierung
all about us

- the Research Group on Law, Science, Technology & Society (LSTS) at the Vrije Universiteit Brussel (VUB), created in 2003
- works predominantly in English
- ca. 60 full-time researchers
- 5 spin-off’s:
  - Brussels Privacy Hub
  - Privacy Salon
  - Brussels Laboratory for Data Protection & Privacy Impact Assessments (d.pia.lab) (2015)
  - Cyber and Data Security Lab (CDSL)
  - Health and Ageing Law Lab (HALL)
- ERC: COHUBICOL (Counting as a Human Being in the Era of Computational Law)
- policy briefs of d.pia.lab
  - 1st (framework) published in May 2017 [EN] [FR] [PT]
  - 2nd (method) published in November 2019 [EN] [FR] [DE] [PT]
  - 3rd (model/template) expected in March 2020 [EN]
context

- ‘tool’ for governance and management of privacy and personal data entangled with their protection and promotion
- ‘tools’:
  - regulatory (legal)
  - organizational
  - technological
  - behavioural

response:
- substantive reasons
  - science & technology development
  - relevance of information in the contemporary society
  - globalization
  - negative experience of the past
  - ...
- formal reasons
  - doubt
  - ethics
  - balancing
  - rationalisation
  - resilience
  - corporate social responsibility
  - procedural justice
  - ...

The Tools of Government
Christopher C. Hood
evaluation techniques

impact assessment

- technology
- environment
- regulation
- health
- privacy
- personal data protection
- surveillance
- social
- ...

- risk appraisal
- value sensitive design
- cost-benefit analysis
- SWOT analysis
- ...

VUB LSTS LAW, SCIENCE, TECHNOLOGY & SOCIETY RESEARCH GROUP
against

- red tape
- limited added value
- instrumentalisation
- **uncertainty** (e.g. ‘black swans’)
- **insufficient** knowledge (e.g. ‘unknown unknowns’)
- ...

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.
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 process
- ...
legal requirements in the EU for D/PIA

- 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 Recital 53 re-use PSI Directive 2019/1024
- 2020 Art 6 ePrivacy Regulation (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.
architecture
<table>
<thead>
<tr>
<th>The framework</th>
</tr>
</thead>
<tbody>
<tr>
<td>2. Considers the relevant societal concerns</td>
</tr>
<tr>
<td>3. Not everything needs it</td>
</tr>
<tr>
<td>4. Uses the appropriate method</td>
</tr>
<tr>
<td>5. Includes recommendations</td>
</tr>
<tr>
<td>7. Relies on sufficient knowledge and know-how</td>
</tr>
</tbody>
</table>
the method for DPIA (GDPR) (1)

1. **Step 1:** Screening if DPIA needed (6 criteria)
2. **Step 2:** Description of processing operations (contextual and technical)
3. **Step 3:** Appraisal of impacts
   - Necessity and proportionality
   - Risks to the rights and freedoms
4. **Step 4:** Consultation with data subjects or their representatives and seeking advice of the DPO
5. **Step 5:** Recommendations: measures to address risks and demonstrate compliance
6. **Step 6:** Prior consultation with DPA
7. **Step 7:** Review

The process flows as follows:
- Start with **Step 1** and proceed to either **Step 2** (Yes) or continue to **Step 4** (No)
- From **Step 2**, if yes, go to **Step 3**; if no, go to **Step 4**
- From **Step 3**, if high residual risk, go to **Step 6**; if no, go to **Step 4**
- From **Step 6**, if no high residual risk, go to **Step 7**; if yes, go back to **Step 3**
- Complete with **Step 7**
the method for DPIA (GDPR) (2)

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
   - *criterion 7: codes of conduct YES/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 DPO

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
authoritative interpretation
why?

- method of regulation: ‘legal hook’
- ...

2012
authoritative interpretation (CJEU)

- ... 
- failure to fulfil obligation 
- action for annulment 
- damages 
- reference for a preliminary ruling 
- ...
e.g. (1) impact assessment & the publics

- public participation in decision-making processes

9. Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.
sample questions

- In what situations would it be “appropriate” to “seek the views of data subjects or their representatives”?
- Who counts as a “representative” of data subjects?
- Can a fee be charged for public participation?
- Is there a legal way to access the contents of a report from the process of DPIA?
- Can a data subject effectively demand to be consulted?
- ...
sample answers

- environmental law
  - environmental democracy
  - environmental impact assessment (EIA)
- ...
any person in the European Community has a right of access to environmental information held by or for public authorities.

the charging of a fee of a reasonable amount is not incompatible with the guarantee of access to information.

fees cannot, however, be fixed at a level which would be such as to prevent the directive from being fully effective.

This would be the case if, due to its amount, a fee were liable to constitute an obstacle to the exercise of the rights of participation.

- [...] **none of the grounds** relied on by the Parliament, considered separately or as a whole, **demonstrates** that it was reasonably foreseeable and not purely hypothetical that **full access to the documents at issue was likely to undermine**, specifically and actually, **the decision-making process at issue** [...].

- However, [...] it remains open to the institutions to refuse [...] to grant access to certain documents of a legislative nature **in duly justified cases**.
authoritative interpretation (ECtHR)

- ... 
- inter-state application 
- individual application 
- opinion 
- ...
Where a State must determine complex issues of environmental and economic policy, the decision-making process must firstly involve **appropriate investigations and studies** in order to allow them to predict and evaluate in advance the effects of those activities which might damage the environment and infringe individuals’ rights and to enable them to strike a fair balance between the various conflicting interests at stake [...].

The importance of **public access to the conclusions of such studies** and to information which would enable members of the public to assess the danger to which they are exposed is beyond question [...].

Lastly, the individuals concerned must also be able **to appeal to the courts** against any decision, act or omission where they consider that their interests or their comments have not been given sufficient weight in the decision-making process [...].
appraisal techniques

7. The assessment shall contain at least:

(a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;

(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

(c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and

(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.
sample questions (GDPR-DPIA specific)

- What exact steps need to be undertaken, by a data controller, in the assessment process, to...
  - ... assess the **necessity** and **proportionality** of the processing operations in relation to the purposes?
  - ... to assess the **risk** to the rights and freedoms of data subjects?

- How the contents (steps) of the necessity test and the proportionality test differ, if ever, between public and private sector organisations, between industry and governance sectors, etc.

- If an aspect of a processing operation has been already assessed against necessity and proportionality, does it need to be assessed also as a risk to the rights and freedoms of data subjects? Or **vice versa**?

- ...
possible answers

- ???
- yet: a trend of **proceduralisation**?
  - **Sweden**: DPA concluded the controller failed to conduct the DPIA process and to consult the said authority (Datainspektionen, DI-2019-2221, 20 August **2019**)
  - **UK**: Heathrow 3rd runway: failure to ”take into account environmental concerns when assessing […] expansion plan” (**2020**)
  - ...


next steps

- **tailoring down** the method to the context of use
  - border management
  - telecommunications industry
  - ...

- **testing** these methods

- analyzing **authoritative interpretation** of legal provisions
  - In **Austria**, DPA rejected a request for prior consultation (Datenschutzbehörde, SB-D485.001/0003-DSB/2018, 18 December 2018)
  - In **Denmark**, DPA rejected a data subject claim that a data controller sent personal data without encryption. The assessment process served as evidence, allowing to conclude that the controller “had made a risk assessment, where the procedure was assessed as an appropriate security measure” (Datatilsynet, 2019-31-1263, 2 July 2019)
  - ...

...
danke schön!

dariusz.kloza@vub.be
@darekkloza
LSTS.research.vub.be
dpialab.org
@dpialab