The automation of privacy- and data protection impact assessments

Dariusz Kloza, István Bőröcz and Marco Giacalone

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

Salzburg, 23 February 2018
Universität Salzburg

21. Internationales Rechtsinformatik Symposium (IRIS) 2018
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

- 47 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

- 1st policy brief of d.pia.lab published in May 2017
Friday, 23 February 2018
Universität Salzburg, Hörsaal 211

16:00 – 16:15  Introduction
16:15 – 16:45  Demonstrations
  ▪ Georg Philip Krog – Signatu (NO)
  ▪ Erwin Rigter – Privacy Company (NL)
  ▪ Robert Sindlinger – OneTrust (DE)
16:45 – 17:00  Evaluation
  ▪ Dariusz Kloza, István Böröcz and Marco Giacalone – VUB (BE)
17:00 – 17:15  Responses
17:15 – 17:20  Concluding remarks
17:20 – 17:30  Public discussion
Part 1: Introduction
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
- ...
Technology at the service of privacy governance & management

- (data) privacy **protection** or **(ab)use** are both a part of its **governance** or **management**

- governance/management for the benefit of the individual → **protection**
  - legal protections
  - organisational protections
  - **technological protections**, e.g. PETs incl. encryption
  - behavioural protections (Kloza 2017: 451-505)

- governance/management for the benefit an **organization** (public & private) → **(ab)use**
  - technology
    - IAPP: Privacy Program Management (PPM) and Enterprise Privacy Management (EPM)
    - NYMITY: Legal Research Software, Privacy Office Support Software, Privacy Management Software
  - ...

... contrast...
A (subjective) retroactive view...
Automation: why particularly now?

- **top-down**
  - regulatory requirements, such as the GDPR in the EU (May 2018)
    - ‘risk-based approach’ triggers resorting to risk management ‘tools’
    - novelties, such as data portability, DPIA, etc. trigger resorting to the use of technology
  - volume of personal data processed
  - difficulty & complexity related to such data handlings
  - (positive?) experience of the IT security & financial sectors
  - limited resources: time, money, manpower, knowledge & know-how
    - ...

- **bottom-up**
  - public awareness, such as the ramifications of data breaches
    - ...

  - ‘privacy technology industry’
    - been around for many years
    - recently: nascent & changing market, but 100+ vendors identified thus far

Some data protection professionals also rely on technological tools to assist them in the DPIA process. For example, both Avepoint and OneTrust offer PIA and DPIA automation tools for IAPP members that can be used to tailor the questions asked to a particular business, flag risks, and generate metrics and reports.

(Fazlioglu [IAPP] 20 Feb 2018)
**Privacy Program Management (PPM)**
- consent managers
- incident response
- website scanning/cookie compliance tools
- data mapping
- privacy assessment managers

**Enterprise Privacy Management (EPM)**
- data discovery
- activity monitoring
- de-identification & pseudonymization
- enterprise communications
- data mapping

Assessment managers tend to automate different functions of a privacy program, such as operationalizing privacy impact assessments, locating risk gaps between data flows and legal regimes, demonstrating compliance, and helping privacy officers scale what have traditionally been complex tasks requiring spreadsheets, data entry, reporting, and so forth.

Source: IAPP, Privacy Tech Vendor Report 2017
Typology (2)

- **Legal Research Software** [legal/regulatory information software]
  - understanding compliance
  - reading the laws
  - staying informed & informing others
  - ...

- **Privacy Office Support Software**
  - building/maintaining a structured privacy program
  - managing a privacy office team
  - benchmarking a privacy program internally and externally

- **Privacy Management Software**
  - D/PIA
  - data mapping/data inventory
  - enterprise assessments
Typology (3) – further criteria

- **software**
  - privately vs. publicly developed; cf. CNIL
  - proprietary vs. open-source; paid vs. free;
  - generic vs. bespoke
  - internally vs. cloud-hosted (SaaS); cf. EU/EEA/CH-hosted vs. hosted outside
  - front-end vs. back-end (modifiable, integrate-able, etc. vs. not)

- **comprehensive package (generic) vs. D/PIA solution only (specific)**

- **addressees (1):**
  - public vs. private sector, or both
  - sector-specific, e.g. health services, local government, …
  - lawyers, ‘privacy professionals’ (e.g. DPO), laymen

- **addressees (2) (product?):**
  - organisation itself → product: software
  - law firm or ‘privacy consultancy’ → products: software & advice

- **aim:**
  - regulatory compliance (e.g. exploitation of data, avoidance of fines, …) vs. beyond (e.g. ethics, social acceptability, reputation, CSR, …)
  - management/governance of data/informational privacy or beyond (cf. typologies of ‘privacy’)

- …
Evaluation criteria

Exhibit 1: Criteria for evaluating PIA guidance documents

2. Discoverability of the Guidance Document
3. Applicability of the Guidance Document
4. Responsibility for the PIA
5. Timing of the PIA
6. Scope of the PIA
   (a) The Dimensions of Privacy
   (b) Stakeholders
   (c) Reference Points
7. Stakeholder Engagement
8. Orientation
   (a) Process compared to Product
   (b) Solutions compared to Problems
9. The PIA Process
10. The Role of the Oversight Agency

(Clarke 2011: 113)

Levels:

1. Regulatory
   1a. Ideal D/PIA
   1b. Arts 35 & 36 GDPR

2. Technological
   2a. Quality attributes (general)
   2b. Specific functionality of the D/PIA software

(NYMITY 2018: 17)

(our own)
Level 1a: 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
9. Deliberative
10. Accountable
11. Assessor is independent
12. Simple
13. Adaptive
14. Inclusive
15. Receptive
16. Grows in supportive environment
Level 1b: Art 35 & 36 GDPR

1. threshold
   ▪ level 1: high risk
   ▪ level 2: specific cases (3)
   ▪ level 3: exclusion list
   ▪ level 4: inclusion list

2. description
   ▪ technical
   ▪ contextual

3. assessment
   ▪ necessity & proportionality
   ▪ risks to the rights & freedoms of individuals

4. stakeholder consultation (when appropriate)
   ▪ due respect for legitimate secrecy

5. contingency plan: measures envisaged to:
   ▪ address the risks
   ▪ ensure compliance with GDPR

6. re-visiting (when necessary)

7. prior consultation
   ▪ high residual risk
   ▪ possible ban of processing

8. DPO consultation
Level 2a: Software quality attributes (general)

ISO/IEC 25010:2011
Systems and software quality requirements and evaluation (SQuaRE) products model

PORTABILITY
- Installability
- Replaceability
- Adaptability

FUNCTIONAL SUITABILITY
- Functional correctness
- Functional completeness
- Functional appropriateness

MAINTAINABILITY
- Modularity
- Reuseability
- Modifiability
- Testability
- Analyzability

PERFORMANCE EFFICIENCY
- Capacity
- Resource utilization
- Time behavior

SECURITY
- Integrity
- Confidentiality
- Non-repudiation
- Accountability
- Authenticity

COMPATIBILITY
- Interoperability
- Co-existence

RELIABILITY
- Availability
- Recoverability
- Maturity
- Fault tolerance

USABILITY
- Operability
- User error protection

Source: www.cse.dcu.ie
Level 2b: Specific functionality

... of D/PIA software
1. discoverability (marketing)
2. vendor/software reputation & trust
   ▪ warranty, maintenance and support, escrow
3. affordability
   ▪ pricing, financial model, cost-efficiency
4. usability
   ▪ “effectiveness, efficiency and satisfaction” (ISO 9241)
5. multilingualism
6. security
   ▪ ‘CIA triad’, protection of personal data, trade secrets, ...
7. intellectual property rights
   ▪ e.g. open access, outsourcing, 3rd party rights

... of D/PIA process within the software
1. process guidance & automation
2. flexible & customizable
3. multi-jurisdictional
4. educative-ness
5. (external) revision/validation/approval
6. audit log
7. reporting
8. data export
Part 2: Demonstrations
Part 3: Evaluation

- comparing apples with oranges
- with a bit of simplification, a 5-point evaluation scale:

<table>
<thead>
<tr>
<th>yes</th>
<th>affirmative</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>negative</td>
</tr>
<tr>
<td>½</td>
<td>in-between</td>
</tr>
<tr>
<td>?</td>
<td>don’t know</td>
</tr>
<tr>
<td>n/a</td>
<td>not applicable</td>
</tr>
</tbody>
</table>
Part 4: Responses
Part 5: Public discussion
Concluding remarks (1)

- the stakes are high
  - “This is not bananas we are talking about.” (Spiros Simitis)
- don’t trust blindly in the automation of anything, incl. that of D/PIA
  - ‘The world gets hung up on automation, partly because it sounds like it saves money, and partly because it saves having to think. It’s the difference between decision systems and decision support systems.’ (Roger Clarke)
  - ‘...under no circumstances should any organisation think it can pass its responsibilities off ... to a piece of software.’ (Roger Clarke)
  - ‘A right to be assessed by a human.’ [provocative] (Niels van Dijk)
- the added value of automation largely depends on the benchmark (template/questionnaire) chosen
“From my experience there is no ‘silver bullet’ in tools for doing DPIA.” (Frank Dawson)

even if you ‘automate’, there is still a lot of room for improvement

- beta versions; continuous development
- need for collaborative development
- integrate-ability between various types of assessments

practical yet essential matters:

- which vendor to trust?
- how to trust cloud-based solutions (security)?

in the EU: verification after 25 May 2018
A wish list: software that...
(under construction)

- ... aids the assessor and not replaces her (i.e. decision-making vs. decision-support)
  - helping discovering problems (risks, ...)
  - suggesting solutions
- ... does not absolve the leadership from accountability
- ... ensures (formal) legal compliance (e.g. necessity, proportionality & risks in DPIA)
- ... offers usable documentation of the D/PIA process (e.g. a report for a DPA; abridged for the public)
- ...
Danke schön!

dariusz.kloza@vub.be
istvan.mate.borocz@vub.be
marco.giacalone@vub.be
@darekkloza
@istvan_borocz
@MarcoGiacalon

vub.ac.be/LSTS
dpialab.org
@dperialb