Vrije Universiteit Brussel
PIAF
PRIVACY IMPACT ASSESSMENT FRAMEWORK
part 1
new tools to protect: pia case-study
PIAF
A Privacy Impact Assessment Framework for data protection and privacy rights
Deliverable D1

Editors:
David Wright, Tri lateral Research & Consulting
Kush Wadhw a, Tri lateral Research & Consulting
Paul De Heni, VUB-LSTS
Dariusz Kliwa, VUB-LSTS

Prepared for the European Commission
Directorate General Justice
JLS/2009-2010/DAP/AG

21 September 2011

PIAF
A Privacy Impact Assessment Framework for data protection and privacy rights
Deliverable D2

Empirical research of contextual factors affecting the introduction of privacy impact assessment frameworks in the Member States of the European Union

Editors:
Gus Hosain, Privacy International
Simon Davies, Privacy International

JLS/2009-2010/DAP/AG
Introduction of PIA policy

- High-level support for PIA
- Compulsory nature
- A firm legal basis
- Conflicts of interest
- Multi-organization and trans-border dimension
- Leadership of the data protection authorities
- Complementary with prior checking
PIA policy: the core elements

• An on-going process
• Scalability
• All privacy types
• Accountability
• Transparency
  – Publication of the PIA report
  – Central registry
  – Sensitive information
• Stakeholders’ involvement
• Risk management
• Audit and review
PIA practice: introduction

• Internal management of PIA
  – Internal architecture
  – Privacy awareness
  – Professional independence of an assessor

• Preliminary issues
  – Threshold analysis
  – Determination of the scale and scope of PIA
  – Roles and responsibilities
PIA practice: the process

1. Early start
2. Project description
   - General description of the project
   - Information flows and other privacy implications
3. Stakeholders’ consultation
   - Identification
   - Information
   - Consultation
   - Consideration
4. Risks management & legal compliance check
   - Risk assessment
   - Risk mitigation
5. Recommendations and report
6. Decision & implementation of recommendations
7. Audit & review
8. PIA is a living instrument
part 2

environmental democracy
privacy is the new green
robin wilton
fundamental rights
deliberative democracy
corporate responsibility
informed decision-making

...
a consultation is a way to gather fresh input on the perceptions of the severity of each risk and on possible measures to mitigate these risks

wright & de hert
<table>
<thead>
<tr>
<th>Features</th>
<th>Australia</th>
<th>Victoria</th>
<th>Canada</th>
<th>Ontario</th>
<th>Alberta</th>
<th>Ireland</th>
<th>NZ</th>
<th>UK ICO</th>
<th>US OMB</th>
<th>US DHS</th>
</tr>
</thead>
<tbody>
<tr>
<td>says PIA is a process</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>contains a set of questions to uncover privacy risks (usually in relation to privacy principles)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>targets companies as well as government</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>addresses all types of privacy (informational, bodily, territorial, locational, communications)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>regards PIA as a form of risk management</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>identifies privacy risks</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>identifies possible strategies for mitigating those risks</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>identifies benefits of undertaking a PIA</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>supports consultation with external stakeholders</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>encourages publication of the PIA report</td>
<td>✓</td>
<td>✓</td>
<td>summary</td>
<td>summary</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>provides a privacy threshold assessment to determine whether a PIA is necessary</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>provides a suggested structure for the PIA report</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>defines “project” as including legislation and/or policy</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>says PIAs should be reviewed, updated, ongoing throughout the life a project</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>explicitly says a PIA is more than a compliance check</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>The PIA policy provides for third-party, independent review or audit of the completed PIA document.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>PIA is mandated by law, government policy or must accompany budget submissions.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>PIA reports have to be signed off by senior management (to foster accountability).</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

piaf deliverable d1
Canadian PIAs seldom involve public consultation, opinion polling or other means of gauging the privacy values of the Canadian public. They tend to focus on legal compliance rather than doing the right thing and asking larger questions.
the final PIA reports often fail to acknowledge ... give it limited berth ... details on such consultations are lacking ... the stakeholders are not adequately identified ...
piaf deliverable d1
most dpas oppose mandatory external stakeholder engagement

- Opposition: 25%
- Support: 18.75%
- Conditional support: 56.25%

piaf deliverable d2
wright & wadhwa
... such an obligation makes sense especially for products and services that will necessarily affect a specific category of people in everyday life: employees, hospital patients, public transport users, etc. ...
4. 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 the processing operations.
access to environmental information
public participation in decision-making
access to justice
aarhus convention 1998
... the importance of public access to ... to information
... the views of individuals were taken into account ...
... individuals must ... be able to appeal to the courts
echr: taskin et al v turkey
aarhus system for privacy?
will the public actually take part?
what is covered already?
additional red-tape?
part 3
co-operation of authorities
European Union - Data Protection Directive
Council of Europe - Convention 108
Central & Eastern European Data Protection Authorities
French-Speaking Association of Personal Data Protection Authorities
Ibero-American Data Protection Network
OECD - Recommendation on the Cross-Border Enforcement of Privacy Laws - Global Privacy Enforcement Network (G PEN)
International Conference of Data Protection and Privacy Commissioners
APEC - Cross-Border Privacy Enforcement Arrangement
Asia-Pacific Privacy Authorities
OEC - Recommendation on the Cross-Border Enforcement of Privacy Laws - Global Privacy Enforcement Network (G PEN)
[Informal Conference]
(1) co-operation within the eu
(2) international co-operation

proposal for the general data protection regulation (2012)
more detailed & specific rules on co-operation
time limits or translation of documents
duty to inform each other
clarity on the extent to which information can be shared

wp29 advice on application art 28(6) of the directive (2011)
mutual assistance
joint investigation
consistency
european data protection board

arts 55-64 proposed general data protection regulation
In relation to third countries and international organisations, the Commission and supervisory authorities shall take appropriate steps to:

(a) develop effective international co-operation mechanisms to facilitate the enforcement of legislation for the protection of personal data;

(b) provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;

(c) engage relevant stakeholders in discussion and activities aimed at furthering international co-operation in the enforcement of legislation for the protection of personal data;

(d) promote the exchange and documentation of personal data protection legislation and practice.
(2)

... the commission shall take appropriate steps to advance the relationship with third countries or int’l organisations ...

art 45(2) proposed general data protection regulation
mutual assistance
investigation or interventions
provide information on law & practice
convention committee

council of europe – proposed modernisation ets 108 (november 2012)
... to organise their co-operation and to perform [their] duties ... the supervisory authorities ... shall form a conference/network ...

art 12bis(8) proposed modernisation ets 108
mechanisms for co-operation within eu
some basis for co-operation with 3rd jurisdictions
some novelties in ets 108
yet certain practicalities still to be dealt with
wp29 & cnil vs. google (2012-)
opc canada & cbp vs. whatsapp (2012-2013)
enforcement co-operation in competition matters
int’l competition network
established october 2001
network of (national or multinational) nca’s
specialized exclusively in competition law
informal
voluntary
project-based
consensus-based
virtual yet structured
procedural & substantive convergence
dissemination of expertise & best practices
facilitation of int’l co-operation & mutual understanding
not a forum of co-operation on individual cases
forum for informal contacts
recommendations & best practices
reports
case-handling & enforcement manuals
templates & toolkits
european competition network
based on regulation 1/2003
created may 2004
co-operation in enforcement of unified rules
efficient division of work between authorities

effective & consistent application & enforcement of law

cohort development of eu competition policy
mechanism for case allocation
rules on conflicts between nca’s and commission
consultation and assistance mechanism within ecn
info on new cases
assistance in fact-finding measures (inspections, interviews)
consultations on envisaged decisions
information exchange (incl. confidential info)
exchange of confidential information
lack of systematic notification on new cases
differences in timetables & investigation procedures
linguistic concerns
time zone differences
formal co-operation complex & time-consuming
little written guidance on co-operation
limits in resources
dpa’s & ca’s – comparable needs & similar obstacles:
(1) practice-oriented approach
(2) limits in sharing (confidential) information
(3) enforcement based on mandatory rules
(4) sharing best practice via informal means
...
part 4

big data
part 5
questions
privacy meeting: brussels – bangalore
cis – bengaluru – 14 august 2013

dariusz.kloza@vub.ac.be
gertjan.boulet@vub.ac.be

vub.ac.be/LSTS
piafproject.eu
phaedra-project.eu
www.cpdpcconferences.org