The state of the art in privacy impact assessment

David Wright

Trilateral Research & Consulting

Warsaw, 21 Sept 2011

The EC is examining…

"An obligation for data controllers to carry out a data protection impact assessment in specific cases, for instance, when sensitive data is being processed, or when the type of processing otherwise involves specific risks, in particular when using specific technologies, mechanisms, or procedures, including profiling or video surveillance"

A comprehensive approach on personal data protection in the EU, COM(2010) 609 final, 4 Nov 2010.

PIAF project

- For DG Justice
- Comprises VUB, Trilateral, Privacy International
- Started Jan 2011, finishes Aug 2012
- Deliverable D1:
  - examines PIA methodologies in Australia, Canada, Hong Kong, Ireland, New Zealand, UK, US
  - 10 case studies (PIA reports)
  - benefits of PIA
  - best elements for construction of a state of the art PIA policy and methodology for Europe
  - legal bases

Definition of privacy impact assessment

- A methodology for assessing the impacts on privacy of a project, policy, programme, service, product or other initiative and, in consultation with stakeholders, for taking remedial actions as necessary in order to avoid or minimise the negative impacts
- A PIA is about identifying risks and finding solutions, not simply producing a report that demonstrates compliance
- A PIA should begin early where there are still opportunities to influence the outcome of a project

Benefits of PIA

- An early warning system, a way to detect privacy problems, build safeguards before, not after, heavy investment – Fix privacy problems now, not later
- Avoids costly or embarrassing privacy mistakes
- Provides evidence that an organisation attempted to prevent privacy risks (reduce liability, negative publicity, damage to reputation)
- Enhances informed decision-making
- A way to gain the public's trust and confidence
- Demonstrates to employees, contractors, customers, citizens that the organisation takes privacy seriously

Elements in good PIA policy & practice

- PIA is a process
- Privacy impact assessment is wider than a data protection impact assessment
- PIA is part of risk management – more than compliance
- PIAs are only as good as the processes that support them
- Mandatory PIAs
- Engaging stakeholders
- Publication of the PIA report
- Third party audits and monitoring implementation
- Tying PIAs to budget submissions
- A central registry of PIAs
- Accountability

For more information

- PIAF Deliverable D1 -- www.piafproject.eu
- Wright, David, “Should privacy impact assessments be mandatory?”, *Communications of the ACM*, Aug 2011
- Wright, David, and Paul De Hert (eds.), *Privacy Impact Assessment*, Springer, 2012 [forthcoming]

- david.wright@trilateralresearch.com