A step-by-step guide to privacy impact assessment

David Wright & Kush Wadhwa
Trilateral Research & Consulting
Sopot, 24 April 2012

PIAF
PRIVACY IMPACT ASSESSMENT FRAMEWORK

Trilateral Research & Consulting

Article 33 of proposed DP Regulation

- Makes PIA mandatory
- Says what a PIA should contain (at least)
  - a general description of the envisaged processing operations,
  - an assessment of the risks,
  - the measures envisaged to address the risks,
  - demonstrate compliance with the Regulation,
- The controller shall seek the views of data subjects
- The Commission may specify standards and procedures for carrying out, verifying and auditing the assessment

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

A step-by-step guide to PIA (1)

1. Determine whether a PIA is necessary (threshold analysis)
2. Identify the PIA team and set the team's terms of reference, resources and time frame
3. Prepare a PIA plan
4. Determine the budget for the PIA
5. Describe the proposed project to be assessed
6. Identify stakeholders
7. Analyse the information flows and other privacy impacts
8. Consult with stakeholders

A step-by-step guide to PIA (2)

9. Check the project complies with legislation
10. Identify risks and possible solutions
11. Formulate recommendations
12. Prepare and publish the report, e.g., on the organisation's website
13. Implement the recommendations
14. Third-party review and/or audit of the PIA
15. Update the PIA if there are changes in the project
16. Embed privacy awareness throughout the organisation and ensure accountability

Template for a PIA report (1)

1. Cover page
2. Executive summary
3. Introduction and overview of the PIA process
4. Threshold assessment
5. Project description
6. Information flows
7. Privacy impacts (risks)

Template for a PIA report (2)

8. Organisational issues
9. Options and alternatives
10. Design features to avoid privacy intrusion
11. Compliance with laws, regulations, codes and guidelines
12. Stakeholder analysis
13. Results of the consultation(s)
14. Recommendations

Do you agree

that the step-by-step guide to PIA and the template for a PIA report meet the requirements of Article 33?

that if an organisation diligently follows the step-by-by guide and the template they would meet the requirements of Article 33?

For more information:

www.piafproject.eu
www.trilateralresearch.com

david.wright@trilateralresearch.com

Trilateral Research & Consulting