Trilateral Research

Respecting privacy rights in the commercial use of personal data

David Wright

Trilateral Research

at the FRA Fundamental Rights Forum

Vienna

23 June 2016

How can privacy by design be better implemented?

- Recital 78 & Art. 25 (adapted):

- to demonstrate compliance with the GDPR, the controller should implement measures that meet the principles of data protection by design and data protection by default.

Examples of measures:

- minimising the processing of personal data,
- pseudonymising personal data as soon as possible,
- transparency re the functions and processing of personal data,
- enabling the data subject to monitor the data processing,
- security features.

Take the principles of data protection by design into consideration in public tenders.

What are the benefits of using certification and seals?

- Art. 42 encourages certification and seals
- An approved certification mechanism may demonstrate compliance with the Regulation
- Seals allow data subjects to quickly assess the level of data protection of products and services
- Voluntary, transparent process
- EDPB may establish criteria for a European Data Protection Seal
- Certification is for three years, subject to renewal
- Certification may be withdrawn if controller or processor no longer meets criteria
- The Board shall collate all certification mechanisms and seals in a register and make them publicly available.

What are the main aspects for a DPIA?

Art. 35: DPIAs are mandatory when

- Processing is likely to result in a high risk
- Automated processing, profiling
- Processing on a large scale of special categories of personal data
- Systematic monitoring of a publicly accessible area on a large scale

Art. 29 WP is considering examples of processing that would and would not require a DPIA

A DPIA is a tool

- for compliance
- for risk assessment
- for consultation

- for competitive advantage (e.g., Microsoft's privacy policy)
- for showing customers that the organisation treats privacy seriously
- i.e., DPIA is a tool for demonstrating respect for privacy rights in the commercial use of personal data

DPIA shortcomings

- Data protection is only one type of privacy
- It is not sufficient for an organisation (company or government agency or CSO) to conduct a PIA or DPIA.
- An EIA is also needed to address non-DP issues such as fairness, inequality, power relations, solidarity, etc.
- Privacy is an ethical issue.

An ethical impact assessment (EIA)

- Process of conducting an EIA is similar to that of a PIA. The two processes could be conducted at the same time.
- A company conducts an EIA to identify ethical risks
- And how to avoid, mitigate, share or insure against those risks
- Desirably in consultation with stakeholders
- Using a code of ethical practice
- May need to alert one or more regulators, DPAs, EUREC.

The most common ethical issues

- the involvement of children, patients, vulnerable populations,
- the use of human embryonic stem cells,
- privacy and data protection issues,
- research on animals and non-human primates.
- avoidance of any breach of research integrity, i.e., avoiding fabrication, falsification, plagiarism or other research misconduct.

- Ethics is given the highest priority in EU funded research: all the activities carried out under Horizon 2020 must comply with ethical principles and relevant national, EU and international legislation, e.g., the Charter of Fundamental Rights and the European Convention on Human Rights

https://ec.europa.eu/programmes/horizon2020/en/h2020-section/ethics

Facebook has initiated an EIA (of sorts)

- *The Guardian*: “Facebook has a new process for discussing ethics. But is it ethical?”, 17 June 2016

Questions

- Who should conduct the DPIA? Staff or external consultant?
- How should we judge the adequacy of stakeholder consultation?
- Who is accountable for adequacy of a DPIA?
- When should the DPIA be publicly available?
- Should the DPIA be subject to an independent, third-party audit?
- Harmonised DPIA vs sector-specific DPIA?
- Should DPAs inspect a random selection of DPIAs?
- Will there be a conflict between an EU DPIA and ISO PIA?

Conclusions

- The EC should prepare guidelines on how to implement Article 35 and foster harmonisation of DPIA, PIA guidelines
- Organisations should be accountable to DPAs for the adequacy of their DPIAs or PIAs
- DPAs should conduct random audits of DPIAs and PIAs
- Default should be to publish DPIAs on the organisation's website
- Organisations should engage stakeholders (internal and external) in conducting PIAs
- EC should interact with ISO re PIA standard
- Organisations should conduct P+EIA – and EC should encourage them to do so.