MINISTERSTWO ADMINISTRACJI I CYFRYZACJI

Data protection impact assessment in the draft General Data Protection Regulation

Boiling the frog: Roundtable on (privacy) impact assessments as a response to (smart) surveillance

Michał Czerniawski
Information Society Department

CPDP 21.01.2015

Broader context: data protection impact assessment as an element of „risk-based approach”

- Privacy (data protection) impact assessment, as mentioned in Chapter IV of the Council's text of the General Data Protection Regulation, constitutes an element of a „**risk-based approach**”;
- At the very foundation of a „risk-based approach” lies **proportionality** – the compliance obligations depend on risk and are **proportional** to the specific processing activities;
- A risk-based approach allows to exercise greater discretion and flexibility in assessing how to address compliance responsibilities;
- However, it is **data controller's duty to demonstrate compliance and to prove that appropriate measures were implemented**.

EU Council's approach 1/2:

- The Council wants data protection impact assessments to be required only for processing activities that likely involve **"high" risk** to the rights and freedoms of individuals, such as **discrimination, identity theft, fraud or financial loss**;

- The requirement to **consult with data protection authorities prior to commencing certain processing activities** (Article 34) is limited to processing that "would results in a high" degree of risk "**in the absence of measures to be taken by the controller to mitigate the risk**";

EU Council's approach 2/2:

- Under the regulation DPIA's aim is to evaluate, in particular, the **origin, nature, particularity and severity of the risk**;

- Regulation, among other things, explicitly states that a DPIA is required for monitoring publicly accessible areas on a large scale, especially when using optic-electronic devices.

Data protection impact assesment: issues

- DPIA generates costs – this may constitute a significant burden for data controllers, in particular SMEs;
- globalisation: issue of data controllers monitoring behaviour in the Union, but with a main establishment outside of the EU;
- the Internet of Things.

How to deal with smart surveillance

- transparency (data subjects allowed to monitor processing operations);
- privacy by design and privacy by default;
- „soft measures”: certification and codes of conduct;
- guidelines issued by data protection authorities, and in the future – by the European Data Protection Board.

MINISTERSTWO ADMINISTRACJI I CYFRYZACJI

THANK YOU FOR YOUR ATTENTION

Michal.Czerniawski@mac.gov.pl