GDPR and its impact

Georges Wantz

21 April 2016

Summary

- What will change ?
- Sanctions
- Processing in the employment context
- Data Protection Officer

What will change ?

- Nothing at all or a lot ?
- Paradigm shift
  - from responsibilities to accountability
  - introduction of obligation of means
- More precisions

Accountability

- Art. 5 par. 2 The controller shall be responsible for and be able to demonstrate compliance with paragraph 1 (of Art 5)
- Art. 7 par. 1: […] the controller shall be able to demonstrate that consent was given […]
- Art. 33 par. 3 (d): the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation […]

Accountability

- The word “demonstrate” is mentioned 16 times in the regulation and 10 times in the preceding considerations part
- It does not only apply to controllers but also to processors

Obligation of means

- Privacy by design and by default
- Data Protection Impact Assessment
- Prior consultation
- Notification of security breaches

Privacy by Design

1. Proactive not Reactive; Preventative not Remedial
2. Privacy as the Default Setting
3. Privacy Embedded into Design
4. Full Functionality – Positive-Sum,
5. End-to-End Security – Full Lifecycle Protection
6. Visibility and Transparency – Keep it Open
7. Respect for User Privacy – Keep it User-Centric

Data Protection Impact Assessment

- Processing likely to result in a high risk for the rights and freedoms of individuals
- prior to the processing
- DPAs will publish lists
- Should at least contain:
  - The description of the processing operations and the purposes of the processing;
  - an assessment of the necessity and proportionality;
  - an assessment of the risks to the rights and freedoms;
  - the measures envisaged to address the risks.

Prior Consultation

- where a data protection impact assessment […] indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk
- prior to the processing

Notification of security breaches

- a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed […] unless the personal data breach is unlikely to result in a risk for the rights and freedoms of individuals
- not later than 72 hours after having become aware of it
- is likely to result in a high risk the rights and freedoms of individuals the controller shall communicate the personal data breach to the data subject without undue delay

More precisions

- Identifiable person
- Consent
- Information to be provided to data subject
- Timelines
- Data portability
- …

Sanctions

- 4% or 20.000.000 EUR for infringements of :
  - Basic principles
  - Data subjects rights
  - Transfers to third countries
  - Orders from DPAs
  - Specific national limitations
- 2% or 10.000.000 EUR for all other infringements

Processing in the employment context

- This will be up to the local legislator to decide

Data Protection Officer

- […]shall designate a data protection officer in any case where:
  - the processing is carried out by a public authority or body[…] or
  - the core activities […] consist of processing operations which […] require regular and systematic monitoring of data subjects on a large scale; or
  - the core activities […] consist of processing on a large scale of special categories of data pursuant to Article 9 and data relating to criminal convictions and offences referred to in Article 9a
- However the considerate (60c) provides for "demonstrating the compliance"

“ Building in privacy might not to be cheap, but just cheaper than building in no privacy”

Thank you for your attention.