Privacy by Design, Security by Design

Dai Davis

Chartered Engineer and Solicitor

Percy Crow Davis & Co

Session ID: PNG 302

Session Classification: General Interest

Privacy by Design

- Original data protection
- New approach
- Draft regulation
- Changes in law
- Changes in enforcement

History of Data Protection Legislation

- Data Protection Act
- 1984
- 1995
- Directive 95/46/EC
- Fully in force since October 2008

Structure of the legislation

- Processing of Personal data
- Registration: from where: how processed: to whom given
- Act in accordance with registration *and* principles
- Obligations on data controller
- In UK: Fewer obligations on data processor
- Individuals' rights - self policing
- Power to issue civil fines up to £½m
- Budget of Information Commissioner

Existing legislation

- Data Protection Act 1998
- Directive 95/46/EC
- Protection of Individuals' Personal Data
- Free Movement of such Data
- European Union legislation
- Inconsistent enforcement
- UK: Large element of self-policing
  - Right of individual to complain
  - Cost of complaining

Fundamentals

- A Regulation not a Directive
- Does not apply to processing by “competent authorities” for … detection … of criminal offences
- Applies where controller or processor is in the European Union
- Also applies where
- data subject is in the EU and
- processing includes “monitoring of his behaviour”

Extra Territorial Reach

- Businesses ≥ 250 employees
- Exemption for “occasional” supply of goods or services
- Must have representative
- In a member state where data subject resides
- For security and design related breaches:
- Maximum fine of 2% of annual turnover

New Data Protection Proposal

- *"The protection of personal data is a fundamental right"*
- Proposal by EU – 25 January 2012
- Simplification of registration system
- Businesses ≥ 250 employees must appoint a data protection officer
- Privacy by design / default
- All consent must be explicit

Extended Personal Data Processing Principles

- Data to be published fairly and in a transparent manner
- Purposes of collection must be specified, legitimate and explicit
- Data processor to prove that consent has been given
- If in a written declaration must be “distinguishable” – e.g. in italics
- No consent if there is a “significant imbalance”

Privacy by Design

- At system design stage ***and*** at time of processing
- “appropriate technical and organisational measures”
- Processing complies with law and
- Ensures protection of rights of data subjects

Privacy by Default - Intention

- Recital
- Data controller should adopt
- internal policies and
- implement appropriate measures
- which meet the principles of data protection by design
- and data protection by default

Privacy by Default - Regulation

- Only process data which it is necessary to
- Not collect data unless necessary
- Not kept for longer than necessary
  - Time and amount
- Limit access to a defined group
- Protect data subjects rights at time of design ***and*** processing
- EU Commission can make subsidiary rules

Privacy by Default - Consequences

- Right to object to data processing
- Right to object to profiling
- Right to be forgotten
  - Requires data *erasure*
- Right to data portability

Information to be provided

- Controller to inform data subject
- Identity and contact details of controller and data protection officer
- Purposes of processing
- Period for which data will be stored
- Existence of right of access and rectification
- Existence of right of erasure or to object to processing

Application - What to do next 1

- Consider how much personal data processing you are doing
- Keep track of the progress of the new law
- It should be passed in ~ one year
- There will be a two year transition period

Application - What to do next 2

- Consider what systems would be effected if you had to:
- Confirm personal data to an enquiring data subject
- Provide some of that data to a competitor?
- Erase that data
- Not profile
- Design systems now that will enable you to do that in the future
- “A stitch in time saves nine”

Privacy by Design, Security by Design

Dai Davis

Chartered Engineer and Solicitor

Percy Crow Davis & Co

Session ID: PNG 302

Session Classification: General Interest