

Are these blocks still solid?



- 1995 Directive, and principles are even older
- Society has moved on:
 - Technology: from mainframe to connected to cloud
 - Data: from static to dynamic to fluid
 - Business: from local-by-default to global-by-default
 - People: from subject to participant
- Do the rules still serve their purpose?

3

Key principles of the Directive



Principle	Translation in the Data Protection Directive
Legitimacy	Article 7: criteria for legitimate personal data processing
Purpose restriction	Art 6: purpose and use restrictions. This includes requirements with respect to data quality/accuracy, purpose specification and proportionality
Security and confidentiality	Art 16-17: requiring measures to ensure the confidentiality and security of data processing Art 8: Special categories of processing (health, religion, race,...)
Transparency	Art 10 & Art 11: the right to information regarding essential aspects of the data processing
Data subject participation	Art 12: right to access, which is typically coupled with the right to correct or delete the data
Accountability	Art. 22-23: rules on remedies and liability Art 28: supervisory bodies

4

Key principles of the Directive



- All still valid and strongly supported!
- But the devil is in the details: how do the principles work?

Let's do a quick review...

5

Personal data and data subjects



- Definition:

“any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity”

6

Not so easy...



→ Recital 26:

“to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person”

→ Opinion WP136 on the Concept of Personal Data (2007):

“One should consider costs, intended purpose, modalities of processing, incentives, interests for the individuals, and organisational/technical risks”

7

Personal data?



IP Information: 83.101.55.109

ISP: schedom vof

Organization: schedom-europe.net european ip range

twitter

YouTube

Search Browse Upload

Add / Remove Modules

Successfully removed. Click here to undo.

Recommended for You

<p>MIB: IL DUE 14 CANTH' ON SOH... 1 year ago 22,205 views [Click here to watch] The Secret Guide...</p>	<p>Livid Rock: Credits Calligayr 2 years ago 1,482,276 views [Click here to watch] PENIS & DORNEX ICTE...</p>	<p>New: MIB in News: Pk-wat X 2012 AL... 15 weeks ago 7,084 views [Click here to watch] The Secret Guide...</p>	<p>American, Mexican Evolution, and P... 1 year ago 62,315 views [Click here to watch] The Secret Guide...</p>
<p>MIB: out for Engineers: How L... 2 years ago</p>	<p>MIB's News: MIB's caught on SO... 1 year ago</p>	<p>MIB's 2012: Behind the History 2 years ago</p>	<p>Disney Hilar: Disney Princesses and W... 2 years ago</p>

Controller versus processor



→ Definitions:

- *Natural or legal person, public authority, agency or other body which alone or jointly with others determines the purposes and means of the processing of personal data*
- *Natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller*

→ Not always obvious:

Purposes *and* means? Joint controllership? Different purposes with multiple controllers?

9

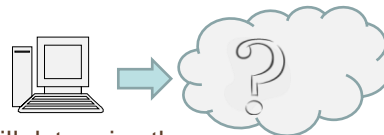
Example - cloud computing: controller or processor?



→ Non-cloud outsourcing: fairly clear:



→ In the cloud?



- Does the outsourcing party still determine the purposes *and* means?
- Does the degree of autonomy of the cloud provider matter?
- Geographic location of data?

10

Applicable law



- Directive, so harmonised across the EU? Not quite...
- Main rule: *each* MS will apply its national law where:
 - Processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State;
 - With multiple establishments for the same controller: each of these establishments must comply with the obligations laid down by the national law applicable
 - Controller is not established in the EU but makes use of equipment, automated or otherwise, situated on the territory of that MS (except when used only for purposes of transit).

11

Effective?



- Directive easily extends to non-EU based controllers
- For global initiatives: multiple MS will claim jurisdiction, and impose different (sometimes contrary) rules:
 - Registration required?
 - Special rules for health care or other sensitive data? Research?
 - Local policy?



12

International data transfers



- Within the EU/EEA: internal market, so no problem
- Outside the EU:
 - Approved 'safe list': Switzerland, Canada, Argentina, Guernsey, Isle of Man, Andorra, Faroe Islands, Jersey
 - Safe Harbor rules for the USA
 - Or contractual frameworks: standard contractual clauses, or Binding Corporate Rules (subject to approval)
- Not a model of effectiveness and pragmatism...

13

Conclusions



- Principles of EU data protection law are still sound
- Application in practice is complex:
 - Need for greater harmonisation
 - Need for more consistent application and enforcement, including across sectors (e.g. gov versus private)
- Main compliance priorities for businesses
 - Even in data protection: think global, act local
 - Conduct your due diligence *before* problems arise...

Questions or comments?



Hans Graux
(m) 0032 (0)479 79 55 00
(e) hans.graux@timelex.eu

time.lex
Rue du Congrès | Congresstraat 35
B-1000 Brussels

(t) +32 (0)2 229 19 47
(f) +32 (0)2 218 31 41

info@timelex.eu
www.timelex.eu