LEIDEN LAW COURSE
LAW & IT IN EUROPE

Privacy and the Protection of Personal Data in Europe

Gerrit-Jan Zwenne ≈ 1 November 2013

Universiteit Leiden
The Netherlands

eLaw Leiden

Leiden University. The university to discover.

roadmap

A. Introduction
   - why do we need a regulation for data protection?
   - the current situation

B. Scope and applicability
   - when does the regulation apply?
   - and to what?

C. Rules for processing personal data
   - what is allowed and what not?
   - what rights have data subjects?
   - third country transfers
   - fines…

why do we need a general regulation on data protection? the current situation

A. INTRODUCTION

privacy law

1948 Universal Declaration (art. 12)
1950 ECRM (art. 8)

fundamental rights and freedoms

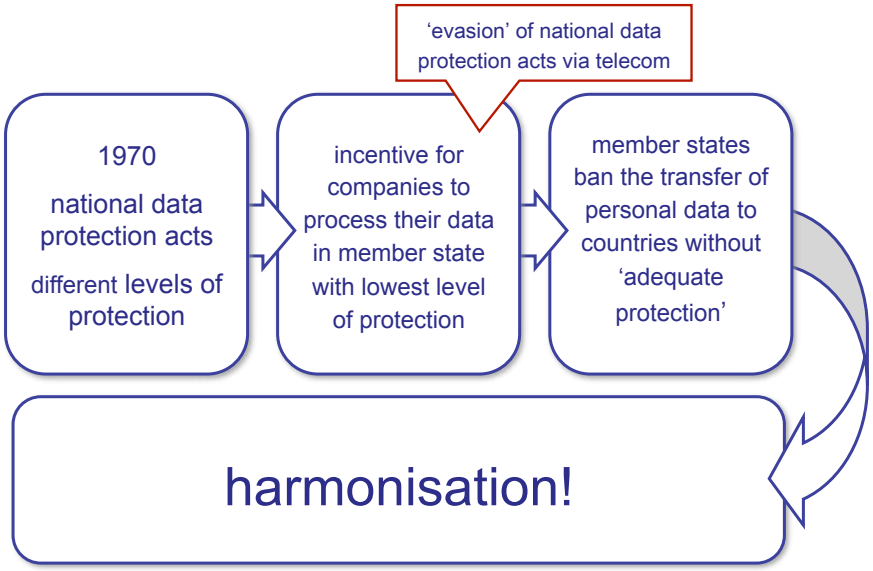
1980 OECD-Guidelines
1981 CoE Convention 108
1995 EC DP Directive 95/46/EC
2014? General Regulation on DP

harmonisation

- *Wet bescherming persoonsgegevens*
- *Data Protection Act 1998*
- *Loi n° 78-17 relative à l'informatique, aux fichiers et aux libertés*
- *Personuppgiftslagen*
- *etc.*

- *EC Version 56 29/11/2011*
- *EC Draft 25 January 2012*
- *EP LIBE draft 21 October 2013*
- *Council….?*
- *…….?*

why do we need a regulation?



legal basis of the regulation

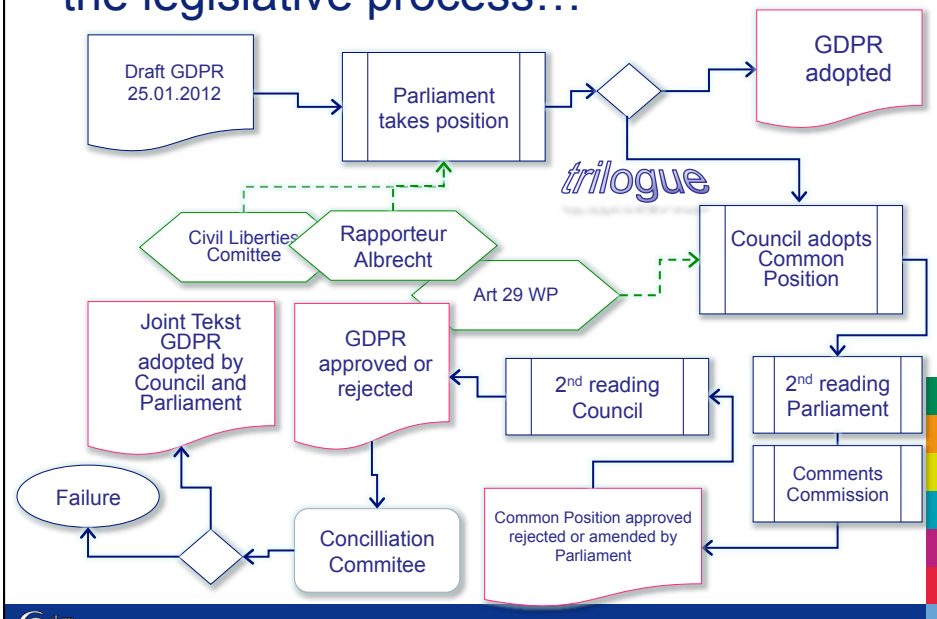
Article 16(2)

The European Parliament and the Council [..] shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. […]

Article 114(1)

The European Parliament and the Council shall [..] adopt the measures for the approximation of the provisions laid down by law, regulation or administrative action in Member States which have as their object the establishment and functioning of the internal market.

the legislative process…



when does the regulation apply? and to what?

B. SCOPE AND APPLICATION

processing of personal data

processing personal data by controllers and by processors

anything that can be done with personal data, incl. collecting, using, deleting, altering etc.

any information about identified or identifiable natural persons (text, image, voice etc.)

also single-out..?

legal or natural person that determines purpose and means of processing (ie the 'owner' of the data)

legal or natural person that processes personal data on behalf of a controller

regulation applies to…

- processing of personal data wholly or partly by automatic means, and
- unless exempted

electronically, ie something with a computerchip: PC, Mac, Blackberry, iPhone, TomTom, setopbox, etc.

- *activities outside the scope of union law (eg. national security), by union institutions, bodies and the like, competent authorities' crime investigations etc.*
- *by natural persons without a gainful interest in the course of their exclusively personal or household activities*

territorial scope…

economic activities: legal entity, branch, office etc.

the regulation applies to:

processing in the context of the activities an establishment of the controller or processor in the union

the entity or natural person that determines means, conditions and purposes of the processing of the personal data

a natural or legal person [..] which processes personal data on behalf of the controller

and territorial scope…

the regulation also applies to processing of union data subjects' personal data by controllers not established in the union, if these processing activities are related to:

- offering of goods or services to such data subjects
- a contract with such data subjects
- the monitoring of their behavior

Facebook, Google, Twitter, etc.

extra territorial effect!

Questions…

Part. 1

1. What EU instrument is currently the basis for harmonized protection of personal data in the union?
2. What is the problem with that instrument? Or, why do we need regulation?
3. What are personal data? Are phone numbers personal data? And IP-addresses? What about photo's? Can sounds or smells be personal data?
4. What activities with respect to personal data do *not* constitute processing of personal data?
5. You try to sell your old iPhone on eBay and in the context of that you process personal data. Would the regulation applicable to that?
6. Philips, a Dutch manufacturer of electronics processes personal data through an ICT-service supplier in India: will this fall under the scope of the regulation? And what if the data-subjects are residents of Beijing?
7. Should Facebook or Twitter comply with the regulation? Why?

what is allowed and what not? what rights have data subjects? third country transfers, etc.

C. RULES FOR PROCESSING PERSONAL DATA

data protection obligations

● *consent* ● *performance of contract* ● *legal obligation* ● *vital interest* ● *public authority* ● *balanced legitimate interest*

- valid basis for processing
- specified and explicit purposes and further processing for compatible purposes
- transparancy and other rights
- security

the purpose of collection determines to what extent further processing is allowed

datasubjects' right to know about the processing of their data

to prevent loss and other unlawful processing

rules for processing personal data

basis for processing
- consent
- performance of a contract
- legal obligation
- vital interests
- public authority
- legitimate interest

purpose of collecting
- legitimate
- explicit and well-defined

retention
no longer than necessary for purpose of collecting

purpose binding
further processing not incompatible with purpose of collecting

processing is allowed

- with unambiguous consent of data subject
  - *sufficient information*
  - *not via acceptance of Terms & Conditions*
  - *not in employer-employee relations*
  - *free expression of data subject's wish*
- necessary for performance of a contract with data subject
  - *including pre-contractual phase*
  - *and everything that is done in the course of a normal contractual relationship (eg newsletter)*

processing is allowed

- necessary for compliance with a legal obligation
  - *eg tax act*
- necessary to protect vital interests of the data subject
  - *life and dead situations*
- necessary for performance of a task carried out in the public interest or in exercise of official authority…
  - *eg tax official*

processing is also allowed…

- if necessary for the purposes of the legitimate interests pursued by controller or by third party or parties to whom the data are disclosed…
- except where such interests are overridden by the data subjects (privacy) interests

- *eg direct marketing, credit management,*
- *fraude prevention*
- *etc.*

need to balance interest, eg by implementing safegurads

collection and further processing

purpose of collecting
- legitimate
- explicit, specific and
- well-defined

needs to provide for a framework within the collection can be assessed

purpose binding
- further processing not incompatible with purpose of collecting

retention
- no longer than necessary for purpose of collecting

consequences for data subjects, from whom data are obtained, sensitivity of the data, similarity of purposes…

special data

- racial or ethnic origin
- sex life
- political opinions
- religious or philosophical beliefs
- trade union membership
- health
- social security number


Baltimore State Hospital
f/t Criminally Insane
att Mr H. Lecter
2000 West Baltimore Street
Baltimore, MD 21223

April 2, 1991, Quantico VA

Dear Dr. Lecter

At the request of.....

Sincerely

Clarice Starling

Questions

Part. 2

8. Someone says: if the regulation applies, consent is required. Is that correct?
9. Can Albert Hein sell Bonuskaart data to health insurers?
10. A court orders UPC to provide to a copyrightholder the subscriber details of ‘uploaders”. What could be the processing ground for the provision of the data?
11. What could an issue if an employer process the employees’ data on the basis of their consent?
12. Can consent be obtained through acceptance of general terms and conditions?
13. How old must someone be to give his/her consent?
14. How could Facebook verify its users’ age?
15. What are ‘special data’ and for what reason provides the regulation for stricter rule for these?

transparency obligations and data subject rights

security breach notification

Article 31 and 32 Regulation

- controller must not later than 24 hours after having become aware of it, notify a personal data breach ~~to the supervisory~~ authority
- in case breach is likely to adversely affect data subject, the controller must inform them without undue delay

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

Questions

Part. 4

16. Suppose you want to know how long a bookshop keeps records of the e-books you purchased. What instruments does the regulation provide?
17. Suppose the bookshop considers this information confidential, as it is essential to its business strategy. For this reason it will not tell you. What could you do?
18. What fines could be imposed on the bookshop?

transfer to third countries

third country transfer only allowed if the non EU-country provides an adequate level of protection

EC Decisions

- US safe harbor principles
- Standard Contractual Clauses

exemptions

- unambiguous consent
- performance of contract
- etc.

transfer of personal data prohibited

third country transfer rules: why?

Article 41 Regulation

inside EU harmonised rules for processing personal data

no data protection related incentives to process data in other member states

more-or-less same level of protection

but still incentives to process data outside EU

outsourcing to 'data havens'

prohibition to transfer data outside the EU, unless…

but publication of personal data on website does not imply 3rd country transfer

even if the data can be accessed from third countries, because…

"given, first, the state of development of the internet at the time Directive 95/46 was drawn up […] one cannot presume that the Community legislature intended the expression transfer [of data] to a third country to cover the loading, by an individual in Mrs Lindqvist's position, of data onto an internet page, even if those data are thereby made accessible to persons in third countries with the technical means to access them"

ECoJ 6 November 2003 Case C101/01

fines

~~100 mio or 2% of annual worldwide turnover~~

a fine up to €100,000,000
or up to 5% of the annual worldwide turnover
(whichever is greater)

Questions

Part. 4

A French automotive company outsources its human resource management system to an Indian service provider. All HR-data will be stored and processed in Bangalore

19. What could to be done to comply with the provisions of Chapter V of the regulation?

Questions

Part. 5

Article 17 of the regulation defines a right to be forgotten. There is some controversy about this right.

20. What arguments *for* and *against* this right can you think of?

@zwnne

questions?

zwenneblog