

LEIDEN LAW COURSE
LAW & IT IN EUROPE

Privacy and the Protection of Personal Data in Europe

Gerrit-Jan Zwenne November 2012



Universiteit Leiden
The Netherlands



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

D. The Right to be Forgotten



EUROPEAN COMMISSION

Brussels, 25.1.2012
COM(2012) 11 final
2012/0011 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)

(Text with EEA relevance)

(SEC(2012) 72 final)
(SEC(2012) 73 final)



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

A. Introduction



privacy law

- | | | | |
|-------|---------------------------------|---|--|
| 1948 | Universal Declaration (art. 12) | } | <i>fundamental rights and freedoms</i> |
| 1950 | ECRM (art. 8) | | |
| 1980 | OECD-Guidelines | } | <i>harmonisation</i> |
| 1981 | CoE Convention 108 | | |
| 1995 | EC DP Directive 95/46/EC | | |
| 2014? | General Regulation on DP | | |

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

- *Version 56 (29/11/2011)*
- *Draft of 25 January 2012*



DP Directive 95/46/EG

basis

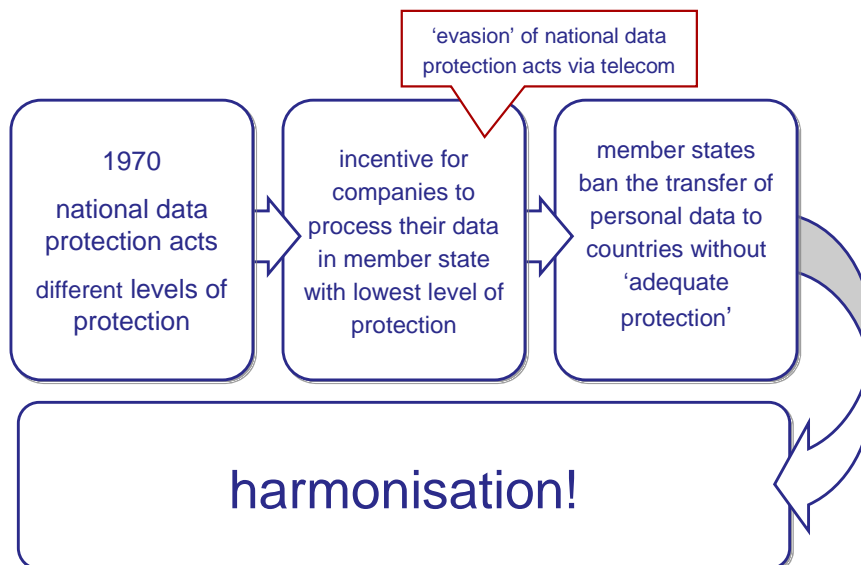
- Art. 95 (100A) EC

objectives

- establishment and functioning of internal market
- ensure a high level of protection for data subjects

.....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

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.



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.)

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

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



regulation applies to...

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



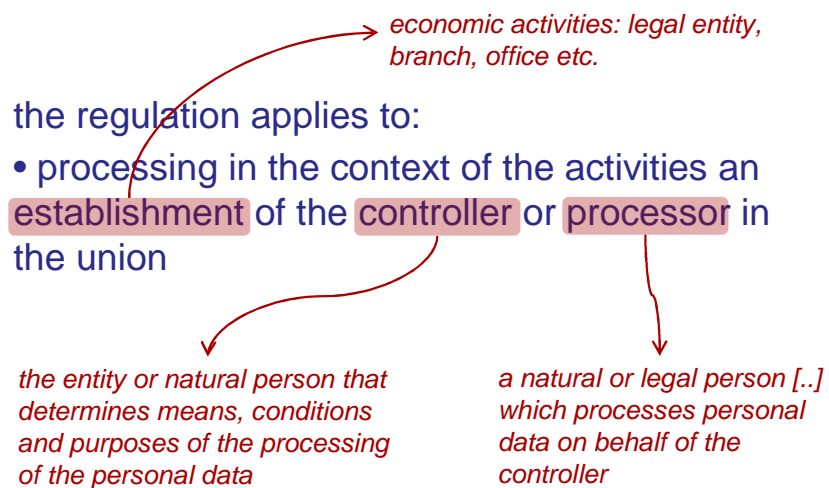
- processing of personal
data wholly or partly by
automatic means, and
- data in a filing system
- unless exempted

structured set of data relating
to different persons

- 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...



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

extra territorial effect!

Facebook, Google, Twitter, etc.

Quiz 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? p What about photo's? Can a sound or a smell 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. Is the regulation applicable?
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
- transparency 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

- unambiguous consent
- performance of a contract
- legal obligation
- vital interests
- public authority
- legitimate interest

purpose of collecting

- legitimate
- explicit and well-defined

purpose binding

- further processing not incompatible with purpose of collecting

retention

- no longer than necessary for 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 **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



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

Quiz 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 copyright holder the subscriber details of 'uploaders'. What could be the processing ground for the provision of the data?
11. What could an issue be if an employer processes 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 a stricter rule for these?



transparency obligations and rights

controllers

- information provision to data subject
- notification to third parties of rectification, erasure etc.
- privacy impact assessments ('PIA') and other documentation
- etc.

data subjects

- access rights
- right to erasure and the right to be forgotten,
- rectification or blocking
- right to object
- dataportability rights
- etc.

security breach notification

- 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

Article 31 and 32
Regulation

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

Quiz 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

in principle, 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...



applicable to websites?

- it is automated processing of personal data
- and the exemptions do not apply
 - public security, defence, State security (incl. economic well-being of the State) and the activities of the State in areas of criminal law
 - a natural person in the course of a purely personal or household activity
 - journalism etc

ECoJ 6 November
2003 Case C101/01



but no 3rd country transfer

ECoJ 6 November
2003 Case C101/01

- 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”




Quiz 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 be done to comply with the provisions of Chapter V of the regulation?



The image shows the phrase "the right to be forgotten" written in a cursive, handwritten style. A red marker is positioned at the end of the text, with a faint shadow cast behind it. The background is white.

D. The Right to be forgotten



“ The Internet has an almost unlimited search and memory capacity. So even tiny scraps of personal information can have a huge impact, even years after they were shared or made public. The right to be forgotten will build on already existing rules to better cope with privacy risks online. It is the individual who should be in the best position to protect the privacy of their data by choosing whether or not to provide it. **It is therefore important to empower EU citizens, particularly teenagers, to be in control of their own identity online**”

Vivian Reding 2012

”



“

...the web is littered with references to my criminal conviction in Italy, but I respect the right of journalists and others to write about it, with no illusion that I should have a 'right' to delete all references to it at some point in the future. But all of my empathy for wanting to let people edit-out some of the bad things of their past doesn't change my conviction that **history should be remembered, not forgotten**, even if it's painful.

Peter Fleischer 2011

”



“

...anyone who advocates the establishment of a full-blown right to be forgotten must clarify what this right means and how it can be effected.

...**considerable obstacles** need to be overcome if people are really to be able to have their digital footprints forgotten and to shun their data shadows

Bert-Jaap Koops 2011

”



“ [The RtbF is] one of the more interesting parts of the Regulation. Its implications for the information society need thinking through carefully – as does the challenge of making this right work in practice. ...

...an insufficiently qualified right to be forgotten could have serious implications for freedom of expression – particularly the right to publish information – and for the maintenance of the historical record.

ICO 2012

”



“ A right to be forgotten wrongly treats freedom of expression as an exception in relation to the right to privacy

Joris van Hoboken 2011

it represents the biggest threat to free speech on the Internet in the coming decade

Jeffrey Rose 2012

Ik schat in dat een dergelijke regeling weinig realistisch is

Corien Prins 2011

”



what's it about?

art. 17(1)
Regulation

claim of datasubjects to have their data
erased and not **further distributed**

can data be
distributed after
erasure...?

- if the data are not longer needed for the purpose of processing
- if the data subject has withdrawn his/her consent
- if the data subject has (successfully) objected to the processing
- if the processing is for other reasons in violation of the regulation

so, what else is
new..?



published personal data

art. 17(2)
Regulation

- if the data are published, the controller has to take measures to inform third-parties about the datasubjects's request for erasure

with respect to the
data published under
his responsibility

incl. links or
references to the data

and if the publishing of the data is done on the
basis of the controllers consent, then that
controller is also responsible for these data



SO...

- when requested to do so the controller must immediately erase the data
- if the data are published **inform** third parties of that request for erasure, and
- if the data are published with his consent, he the controller is also responsible for these data

do-no-remember-register..?

filters? blacklists of embarrassing photo's?



exceptions

- Right to be Forgotten*
- no **RtbF** if data that are needed
- for exercising the right of freedom of expression
 - for reasons of public interest in the area of public health
 - for historical, statistical and scientific research purposes
 - for compliance with a **legal obligation** to retain the personal data

- *objective of public interest*
- *respect essence of the right to protection of personal data, and*
- *proportionate to the legitimate aim pursued;*



further

- delegated acts
 - second category fines
 - unknown administrative burden
- European Commission
- max. €500.000, or
 - 1% worldwide turnover...



a suggested alternative

Article 17a Notice and take down

Where an information society service provider processes personal data other than as the controller of such data, the information society service provider shall provide the data subject with easily accessible means to request the personal data to be removed from the service, [especially where the data relate to the period during which the data subject was a child]

'any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of the services' (2000/31/EC)

VNO-NCW
October 2012

Quiz 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?



twitter
#eLaw

questions?

zwenneblog • gerrit-jan.zwenne@twobirds.com • @zwnne