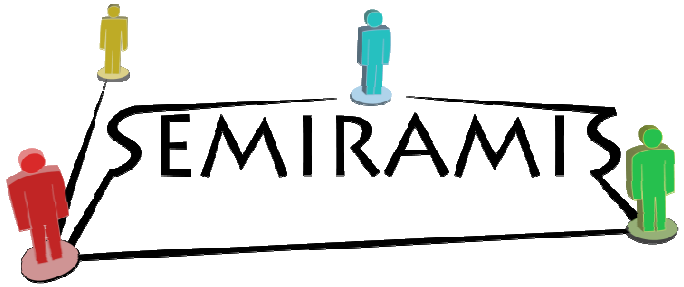

Secure Management of Information across multiple Stakeholders

Data Protection Reform

Javier Sempere Samaniego

Head of Legal Department

Data Protection Authority of the Region of Madrid

Why?

- Wrong transposition of Directive 95/46
- Same rules for companies
- To adequate to technology
- To reduce administrative tasks
- To increase protection of data subjects with new rights
- To introduce new “data protection instruments”

Scope

Directive 95/46:

- Establishment of controller in UE
- Controller outside of UE:
  - But national law applies according to international law
  - Equipment or data bases are in UE

New Proposal:

- **Introduces “Territorial scope”**
- **Controller outside of UE and:**
  - **Offering services and products to data subject UE, or**
  - **Monitoring their behaviour**

New rules to protect data subject (1)

- **Data subject consent**

  Directive 95/46: “any freely given specific and informed indication by which data subject signifies his agreement to personal data processing”

  Transposition: express or tacit

  New regulation: by an statement or by a clear affirmative action; not to avoit tacit consent

New rules to protect data subject (2)

- **Right to be forgotten:**

New right?

How to apply this right to…?:

- social networks
- “official gazettes”
- websites
- newspapers

Exception: not to apply in case of freedom of speech or public interest

Which is the responsability of internet search engines as google?

New rules to protect data subject (3)

- **Right to data portability:**

  “personal data processed by electronic, to obtain from the controller a copy of data”

  Data subject can transfer its personal data in electronic format

- **Right of access and Right of information:**

the period for which the personal data will be stored

Controllers obligations:

Not to notify databases to DPA's but…

To mantain the following documentation:

- Description of data base
- International transfer
- Who is the data protection officer
- Period to delete personal data
- Contract with processor

Also:

To cooperate with DPA

To adopt security measures

To notify security breaches

New obligation for controllers: To notify security breaches

- Compulsory for telecommunications companies (directive 2002 electronic communications)

To communicate:

to DPA (24 hours) including measures adopted

to data subject

Which is the purpose of this communication?

Sanction by DPA?

Legal framework for International Transfers:

- Exceptions: consent by data subject; performance a contract; necessary for public interest

- Third country with adequate level

- Binding Corporate Rules (passed by DPA)

- Standard data protection clauses adopted by EC

- Standard data protection clauses passed by DPA

Data Protection Officer

- Compulsory to:

- Public Administrations
- Companies with more than 250 workers

- Characteristics:

Expert on data protection

Tasks related to data advice

Independence status

To communicate his/her appoinment to DPA

2 years (with the possibility to extend 2 years more)

Economic sanctions:

-**Not all DPA's impose economic sanctions:**

Spain: only to private companies yes, public sector not

Uk: private and public sector

Another countries: neither private companies nor public sector

- Fines:

250.000€ or 05%: not comply with data subject rights

500.000€ or 1%: not comply with duty of conservation documents

1 million€ or 2%: not comply with PIA or notification data breach

Another issues:

Privacy Impact Assesments (PIA)

Privacy by design and by default

European Privacy Seal

European Data Protection Board

Merci!
Thank you!

javier.sempere@madrid.org