Privacy in the Workplace – PAW Project

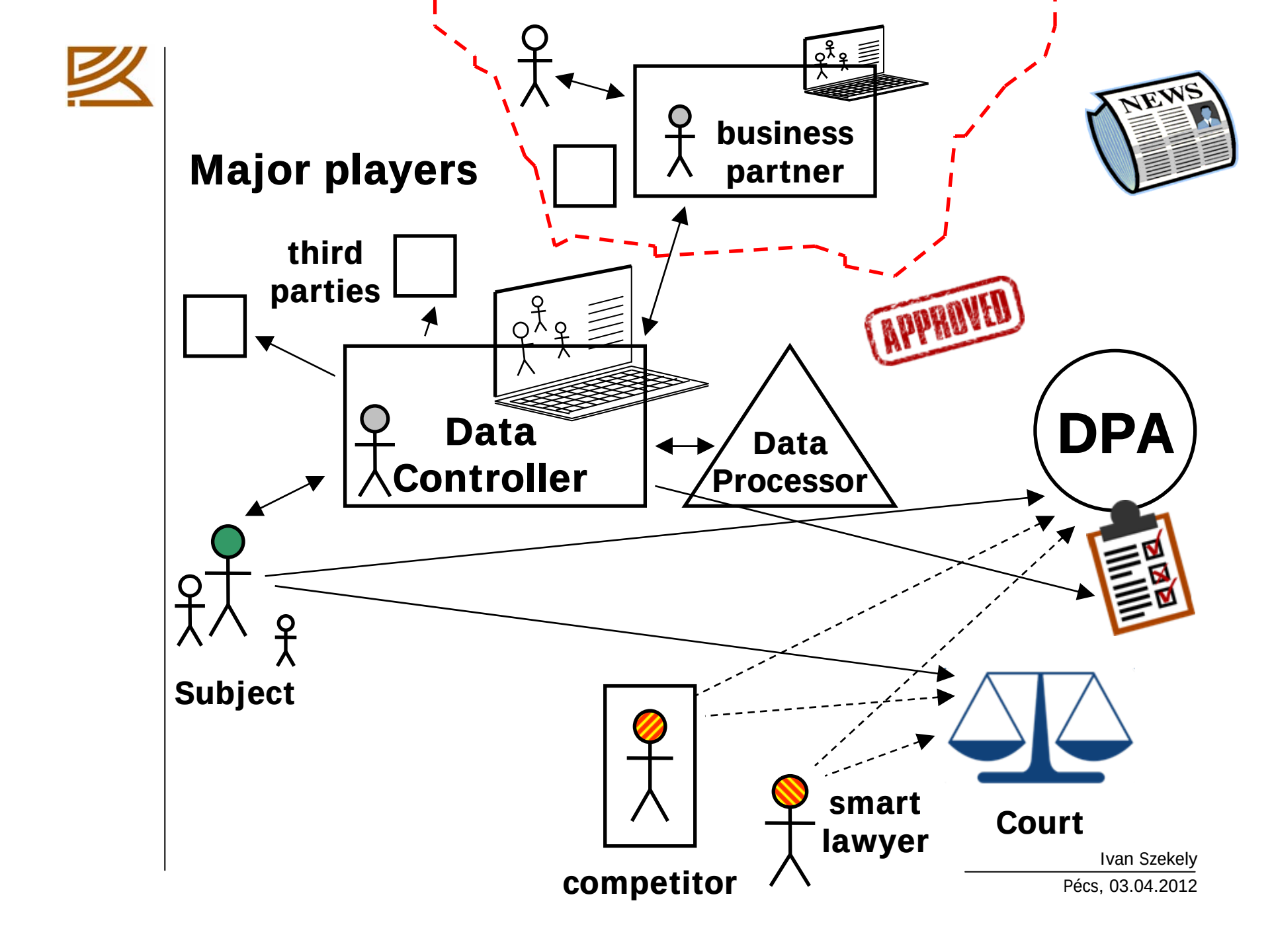
Auditing, investigating, or giving professional advice?

Consulting experiences with data controllers in Hungary

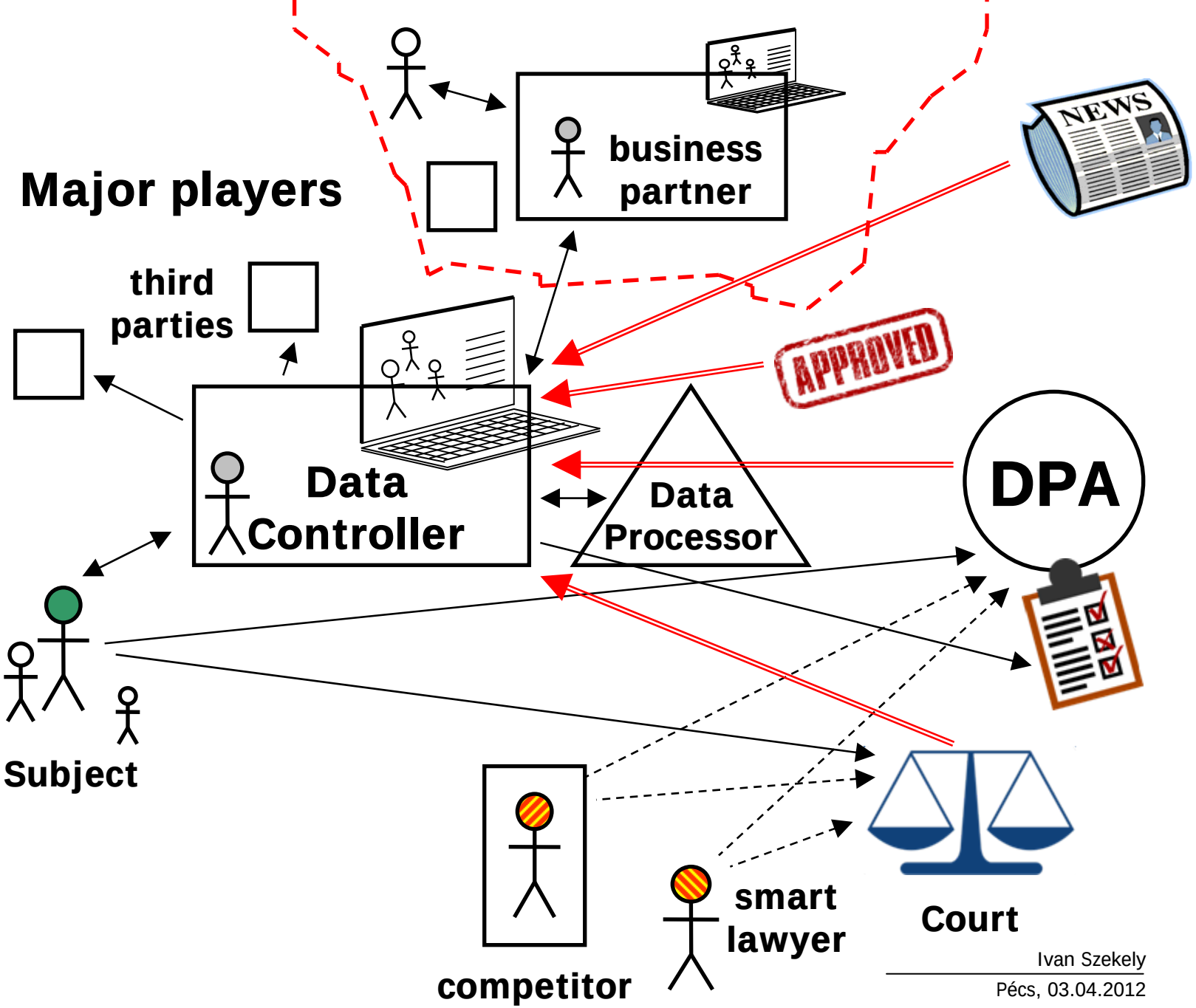
Dr. Ivan Szekely
szekelyi@ceu.hu

PAW International Conference
Pécs, 2–3 April 2012

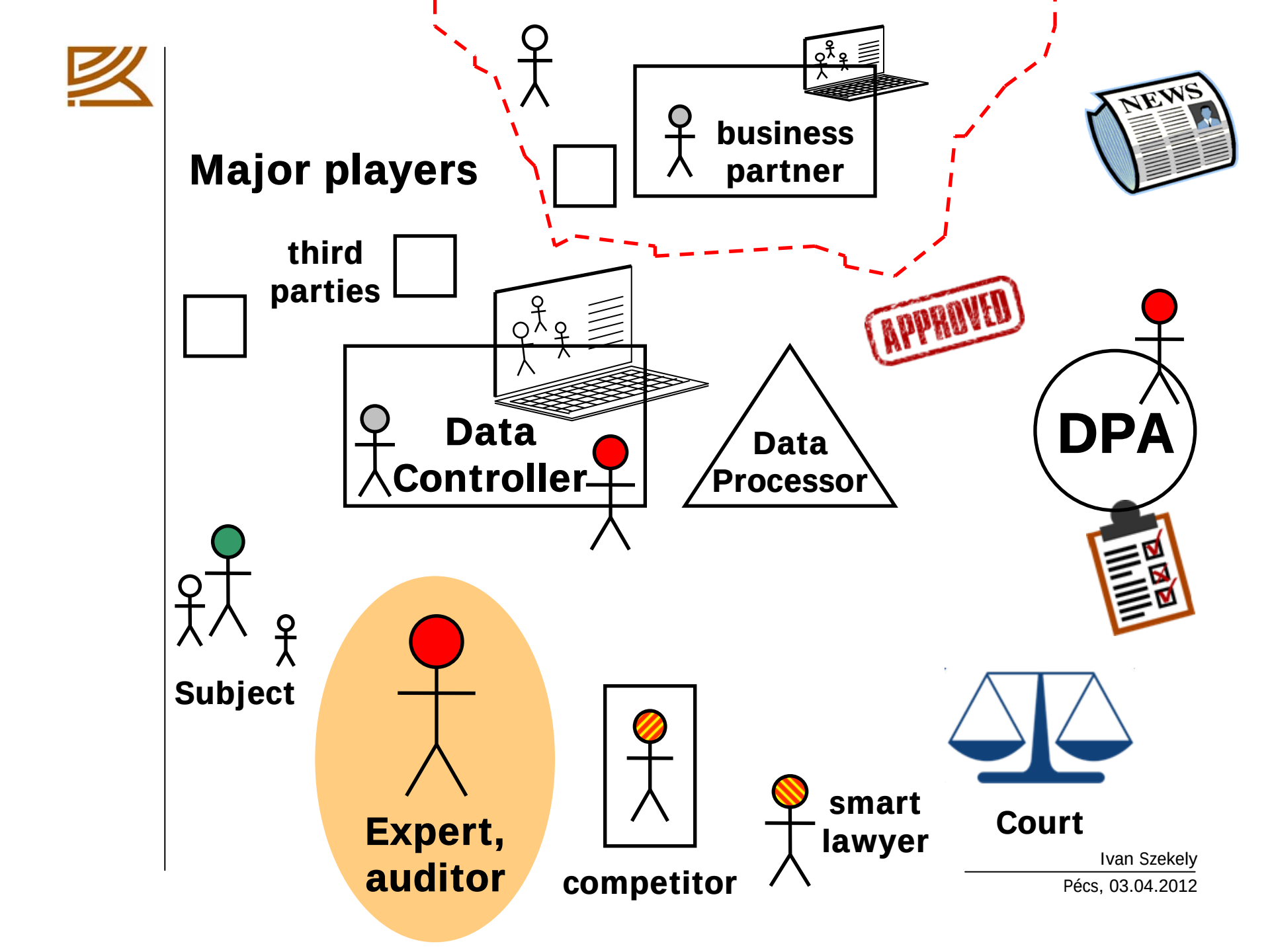
Major players



Major players



Major players



Ivan Szekely

Pécs, 03.04.2012

Major periods

A. The change of the political system

B. The mid-nineties

C. The new millennium

D. 1 January 2012 –

Major periods – The change of the system

Reasons: Weakened legitimacy of data controllers
Constitutional Court decisions
New large data controllers
DP-FOIA

Methodology: Observations derived from principles
Compliance with legal provisions

Conducted by: Individual experts
Law firms

Major periods – The mid-nineties

New component: Investigations of the Parliamentary Commissioner (DPA) (complaints or *ex officio)*

Methodology: Complaints – answering only the question asked

Ex officio – legal compliance, data subjects' rights

Conducted by: Public servants from the office of the DPA

Major periods – The new millennium

Reasons: Increased activity of supervisory authorities
Legal remedies of data subjects
Increased political sensitivity of data processing
Awareness of data controllers

Clients: Large private data controllers
"Electronic government"

Methodology: Higher professional standards, more practical

Conducted by: Specialized teams of experts
Law firms
Units of large auditor firms
Consortiums

Major periods – From 1 January 2012

- New component: New data protection act
  New DP Authority
  New audit provisions

Clients: ?

Methodology: ?

Conducted by: Public servants from the office of the DPA (?)

Audit, examination, advice, consultation?

Audit:
- formalized methodologies
- specialized auditing organizations
- resulting a qualification or ranking
- results are public

↳ Conflict of interest: *internal*

(employees or interested partners cannot participate)

Audit, examination, advice, consultation?

- Examination or “screening”:
  - similar principles but different methods
  - non-specialized organizations; experts
  - resulting a report and suggestions
  - confidentiality clauses

    ↳ Conflict of interest: *external*

    (employees of supervisory authorities cannot participate)

Hungary 1989–2011

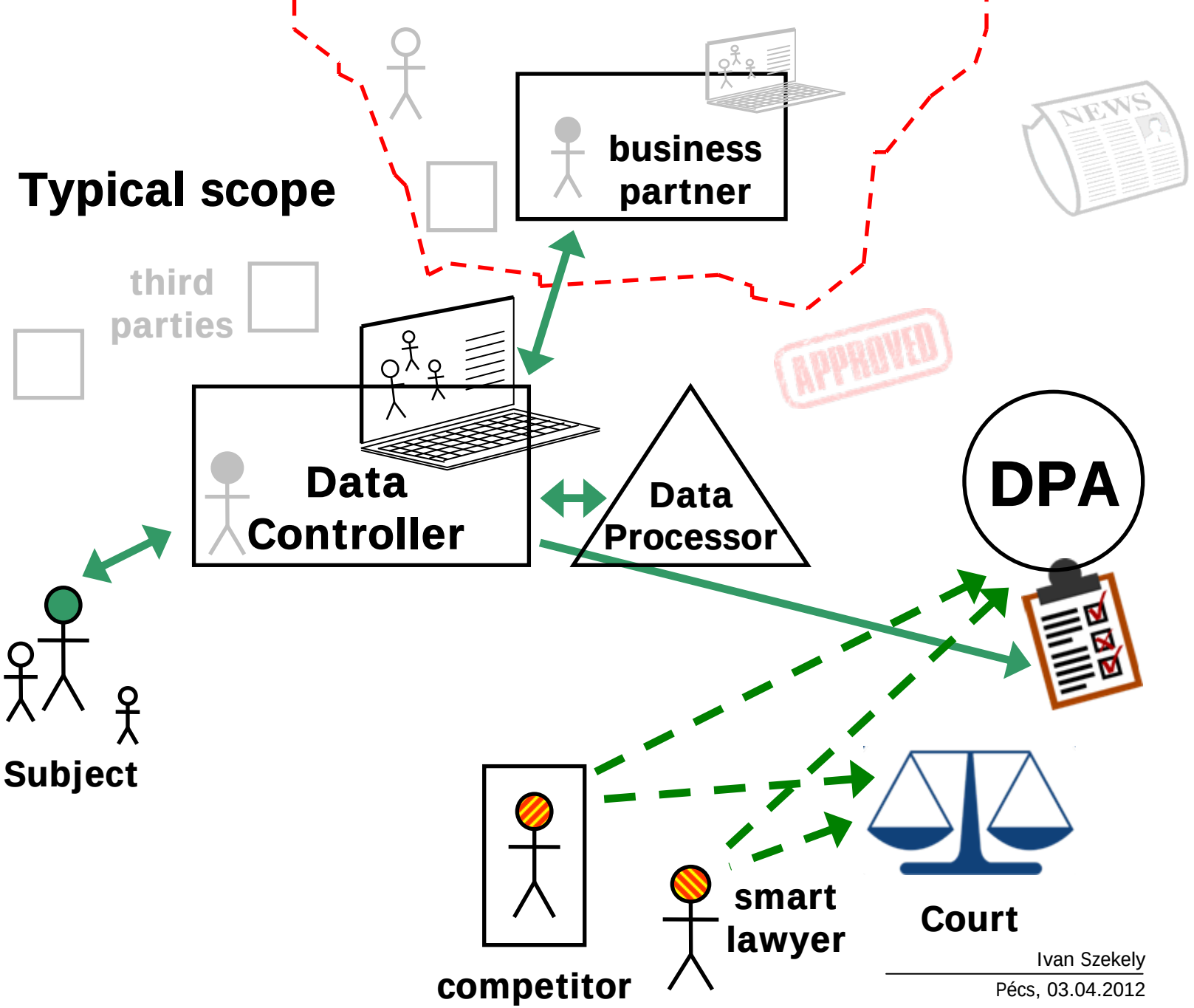
- Only data protection examinations/screenings with certain functions of auditing
- Formalized methodologies: only of limited use
- Different problems and expectations
- Different data controlling systems
- Individual cases

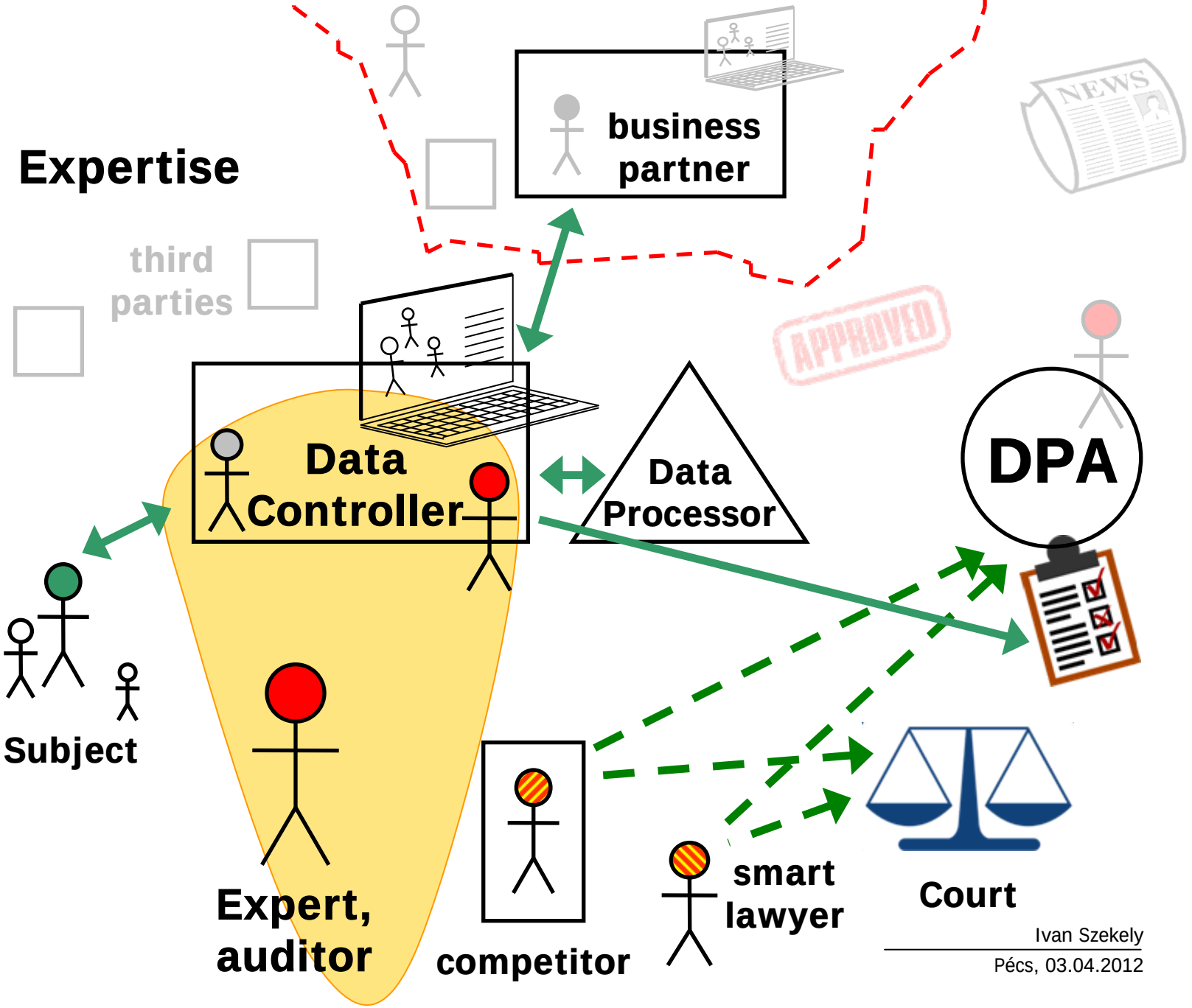
Examination / screening categories

- Basic level screening: examines general compliance, identifies sensitive issues
- Medium level screening: covers all areas of data processing, provides suggestions for *certain* issues
- Detailed screening: covers all areas of data processing, provides suggestions for *all* problematic issues

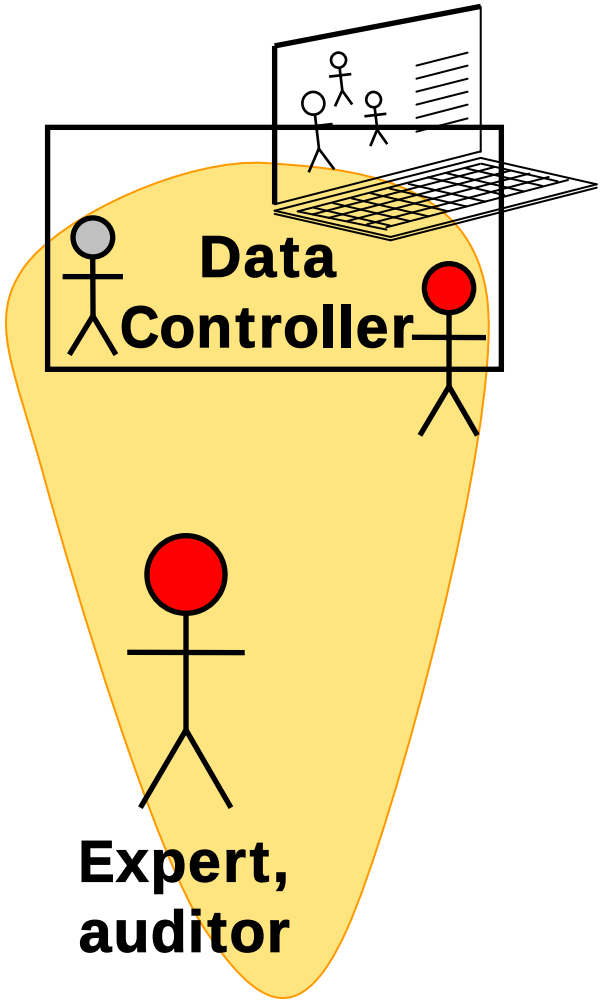
↳ Conducted by carefully composed teams of experts

Typical scope




Expertise
business partner
third parties
NEWS
APPROVED
Data Controller
Data Processor
DPA
Subject
Expert, auditor
competitor
smart lawyer
Court

The necessary expertise

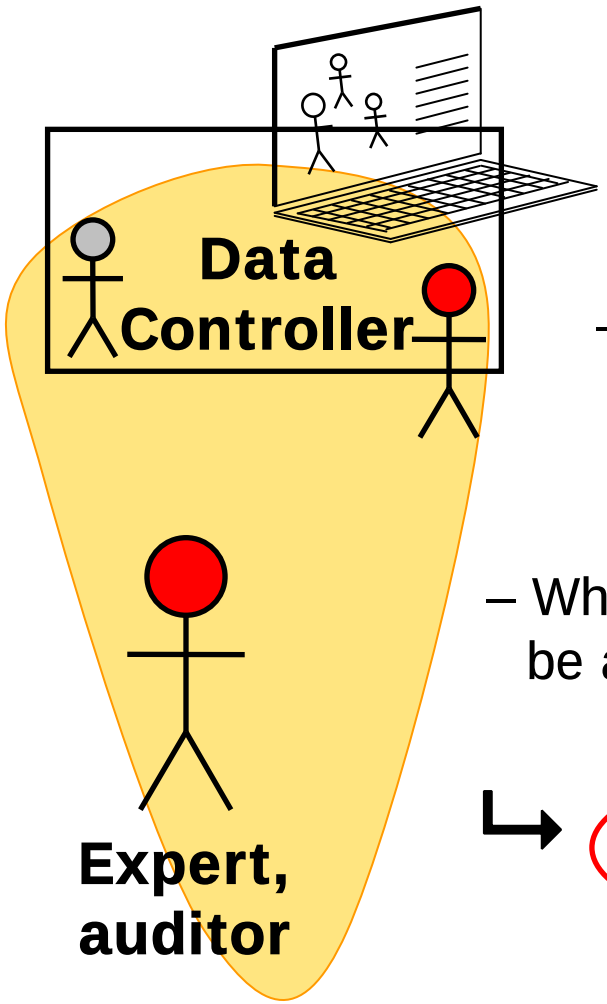


- Internal + external expertise
- Collaboration of internal + external participants
- Confidential relationship, secrecy
- The role of the internal data protection officer
- The significance of the composition of the auditing team

Typical problems

During the examination of:

- products
- processes
- regulations and other documents
- the IT system
- etc.

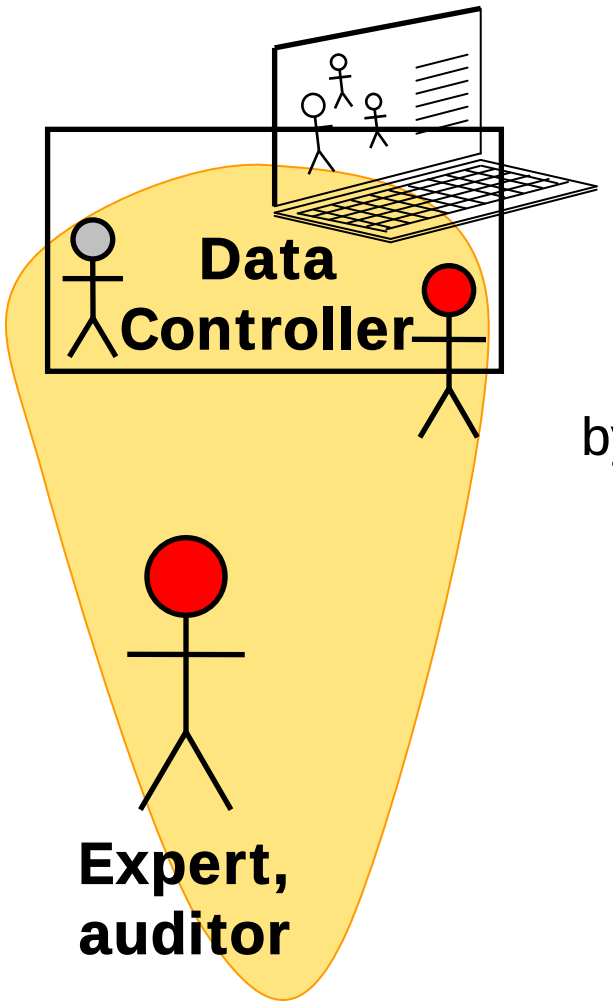


– Too much documents need to be browsed from DP aspects (documents are not categorized)

– What documents, declarations can be accepted as equivalent to reality?

↳ Documentation = Reality?

Misconceptions



by the Client:

- Hiding facts from the auditor
- Active defense, attacking
- Passive disobedience
- In the US it is different...

by the Auditor:

- we are experts in everything
- data protection =
  “protection of the data”
- IT examination =
  data security audit

Suggested methods

(among others:)

- Document analysis
- Interviews
- On-site examination
- Examination of Data Controller’s authorizations, licenses
- Checking of customer relationships
- Establishing of test customer relations
- Testing of remote customer relations (online, offline)
- Examination of the IT system
- etc.

Suggested aspects

(among others:)

- Regulation and documentation of internal data processing procedures
- Relations among business processes, business logic and data protection requirements
- Compliance with legal provisions
- Contacts with data subjects, possibilities of their exercising of rights
- Connections with data processors, other data controllers
- etc.

Crucial point: the IT system

Usual problems:

- Data flows do not follow the legal procedures
- The management does not understand information technology
- IT professionals deceive business management
- Business management and IT professionals deceive the auditors
- Documentation does not reflect reality
- The auditor does not understand the IT system
- The auditor understands data security only

Minimum requirements of the reports

- Description of the existing status of the data processing system
- Evaluation of certain elements, good and bad solutions in the data processing system
- Drafting of suggestions for improving the status of the data processing system

The right order of the products

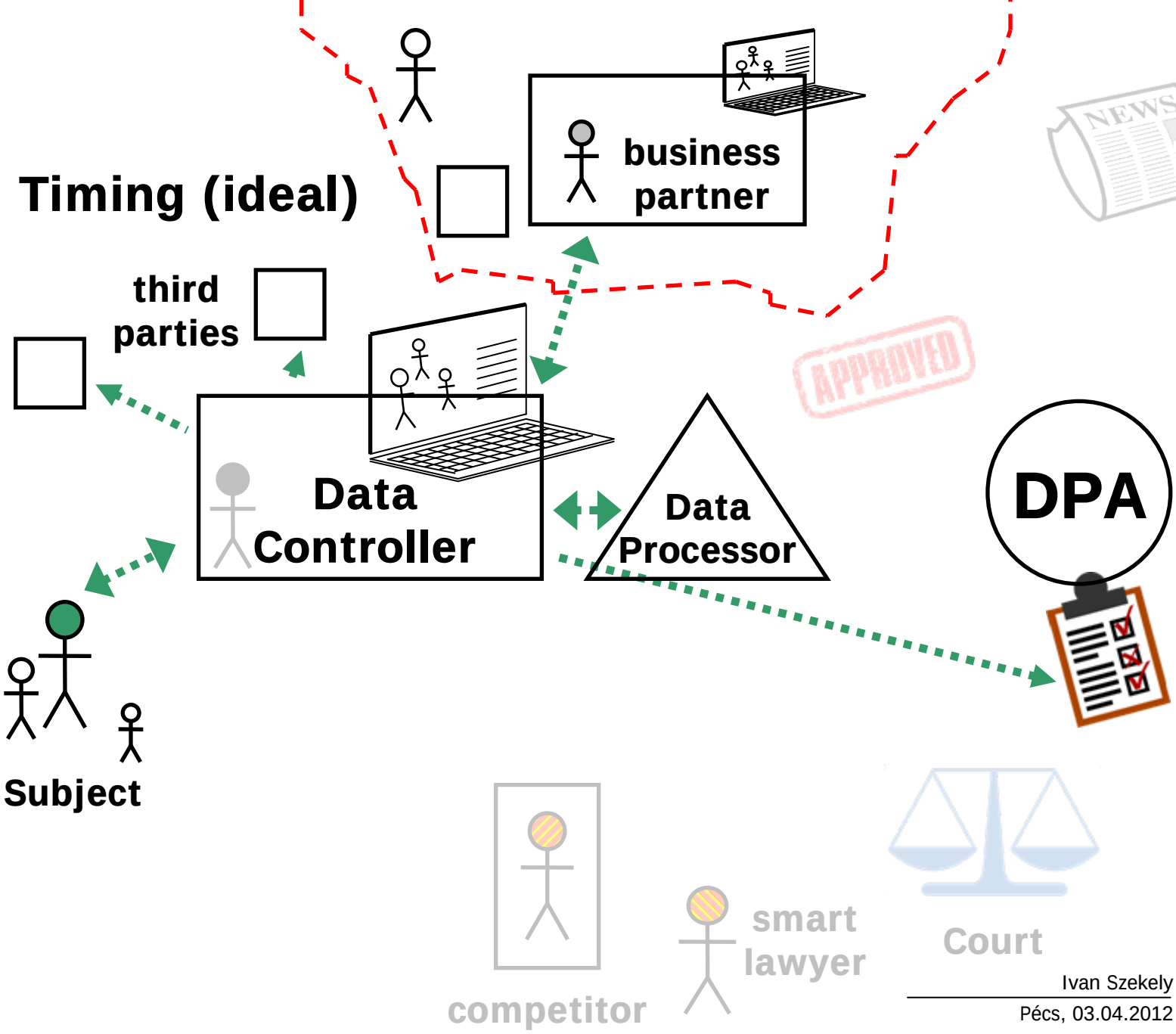
1. Examination / screening

2. The Report

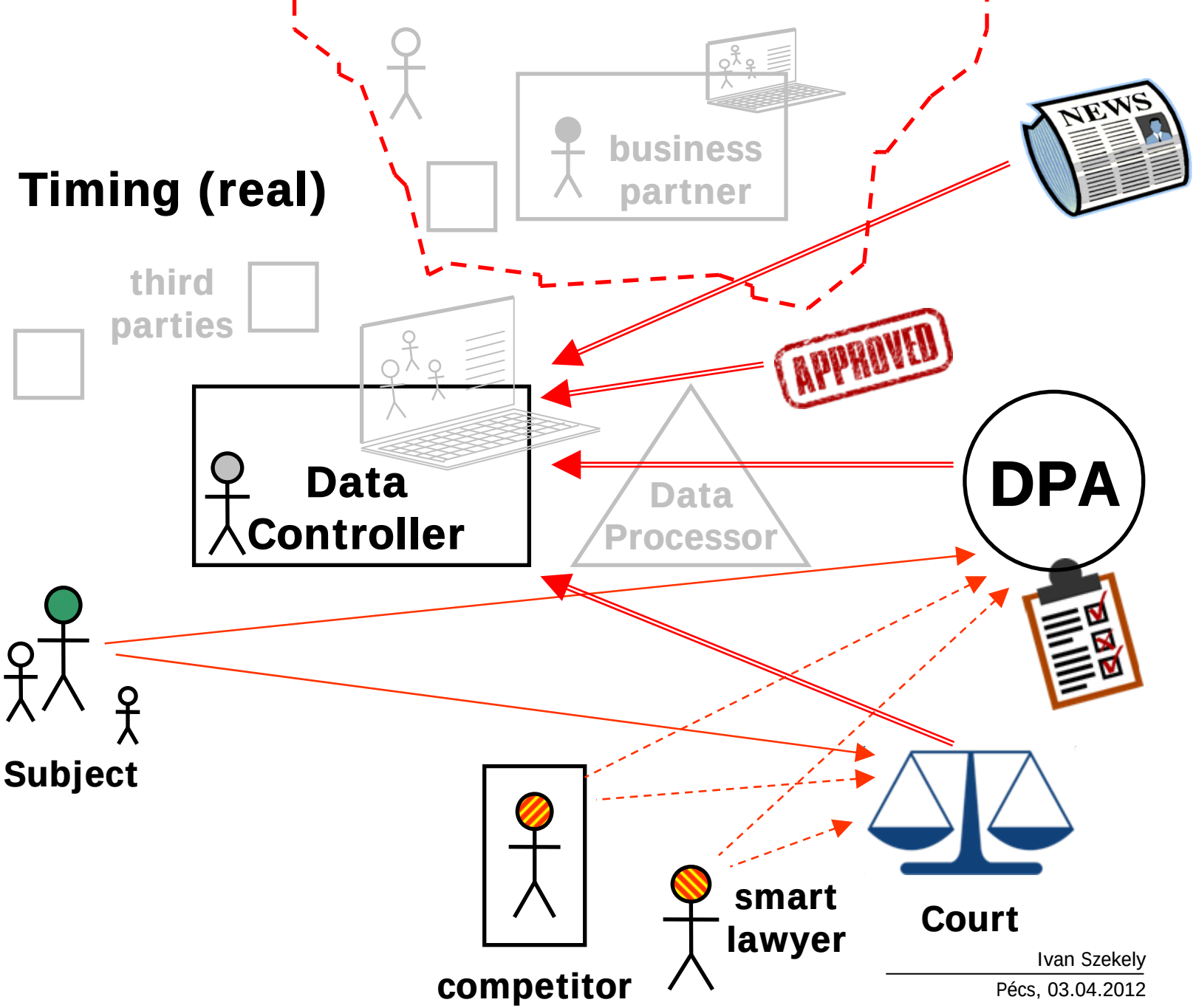
3. Internal data protection regulation

4. Privacy Policy (public)

Timing (ideal)



Timing (real)


business partner
NEWS
third parties
APPROVED
Data Controller
Data Processor
DPA
Subject
competitor
smart lawyer
Court

Ethical dilemmas

- May the expert/auditor suggest “grey” solutions?
- The expert/auditor is neither a virtual judge, nor an ombudsman (rather a virtual lawyer helping the client)
- The expert/auditor must set aside his value judgments (but where is the limit?)
- May the expert/auditor criticize other experts/auditors?
- The results of the examination may end up in the safe
- The client can selectively publicize the expert/auditor’s observations

Overall conclusions

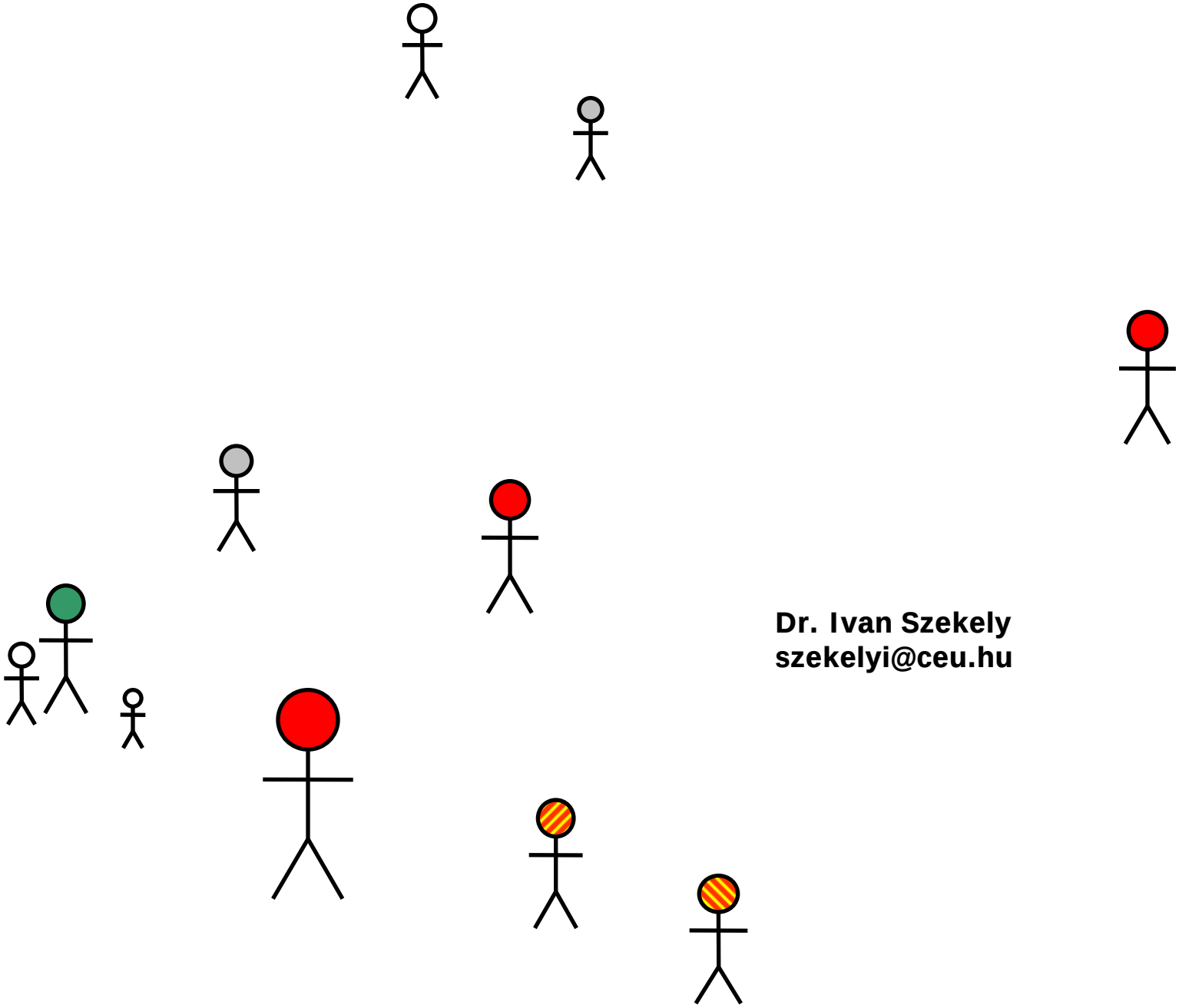
- It is a complex task; specialists or teams must have a complex expertise
- A systemic approach is needed
- *Data protection* IT audit should be included
- A snapshot – regular monitoring is necessary
- A good internal DP officer can be of much help

Open questions

- Will data controllers behave in an unreserved manner towards the auditors of the DPA?
- Can data controllers get a certification for their future operation?
- Will a formally audited data controller have advantages when submitting complaints against the data controller?
- Will the data controller go to court if it will be sanctioned despite a former audit?

Open questions (contd.)

- Will the DPA outsource its auditing activity in case of mass demand?
- Will the DPA accept the results of former examinations/screenings conducted by others?
- Will data controllers have both “official” and “private” audits conducted?
- Will court practice be influenced by the existence and results of official audits?
- ...



Dr. Ivan Szekely
szekelyi@ceu.hu