Joint controllership: upcoming guidelines and case study

Veronique Ciminà
Owe Langfeldt

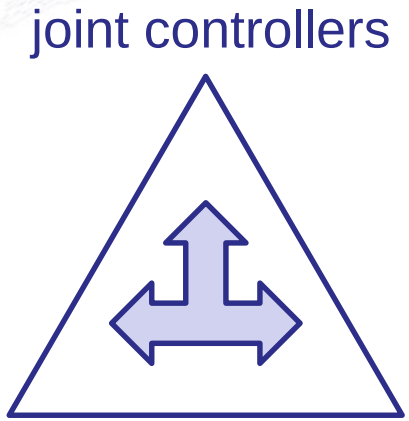
DPO-EDPS meeting at EIOPA
17/05/19

Life, the Universe and Everything... ... almost

- Upcoming EDPS Guidelines on joint controllership (... and related things)
- Case study: WEED^2 system
- Conclusion

Upcoming EDPS Guidelines

- Why?
  - "Accountability follows the controller"
    - so who controls what?
  - New specific rules in Art. 28
  - Recent case law (Wirtschaftsakademie, Fashion ID, Jehovah's Witnesses)
- Scope:
  - joint controllers (main focus)
  - controller-processor
  - transfers between separate controllers
  - Systems with MS involvement
  - FAQs, example cases, checklists...



Upcoming EDPS Guidelines

- Timeline
  - Draft chapter on joint controllers: sent to you for comments on 13/05/19 – please provide comments by 06/06/19
  - Full draft for comments: scheduled 06/19
  - Scheduled adoption: 07/19
  - NB: EDPB is working on controller/processor opinion (updating WP29 1/2010), public consultation before summer, adoption autumn

Joint controllers (Art. 28 EUDPR)

- JCs can also include non-EUI entities, e.g. MS authorities.
- Assignment of roles by Union legislation, or if (and so far as) not, by arrangement between JCs;
- Form: not defined;
- Transparency of arrangement:
  - ‘essence’ of the arrangement made available to DS, e.g. in data protection notice;
  - mention JCs in records (related: all JCs need to keep records).
- ‘Joint’ does not mean ‘equal’!

Case Study: WEED^2

Case study: WEED^2

- The *Very Important EU Institution* (VII) and three *Quite Important Agencies* (QIA) want to better cooperate by pooling information on drug abuse in the EU, which would also include personal data about health effects of drug abuse. They have a legal basis to do so.
- To this end, they want to set up the *Wondrous European Extra-legal Drug Database* (WEED^2).
- VII's Drug Research Understanding Group (DG DRUG) and the QIAs will each use the information for their related tasks, but want to be able to control others' access to their information.

Case study: WEED^2

- VII will run WEED^2, using its own IT department (DG TECH) as a provider. DG TECH often uses IT-CORP as a hosting provider.
- VII DG DRUG and the QIAs decide on the direction of the project in a Steering Committee (SC) chaired by DG DRUG.
- The SC will define the functional and non-functional requirements for WEED^2.
- The system will be built by VII DG TECH, based on the instructions received from the SC.

Case study: WEED²

VII

DG DRUG
chairs SC
uses WEED² for its own tasks

DG TECH
provides WEED²

IT-CORP
hosting provider

QIA1
uses WEED² for its own tasks

QIA2
uses WEED² for its own tasks

QIA3
uses WEED² for its own tasks

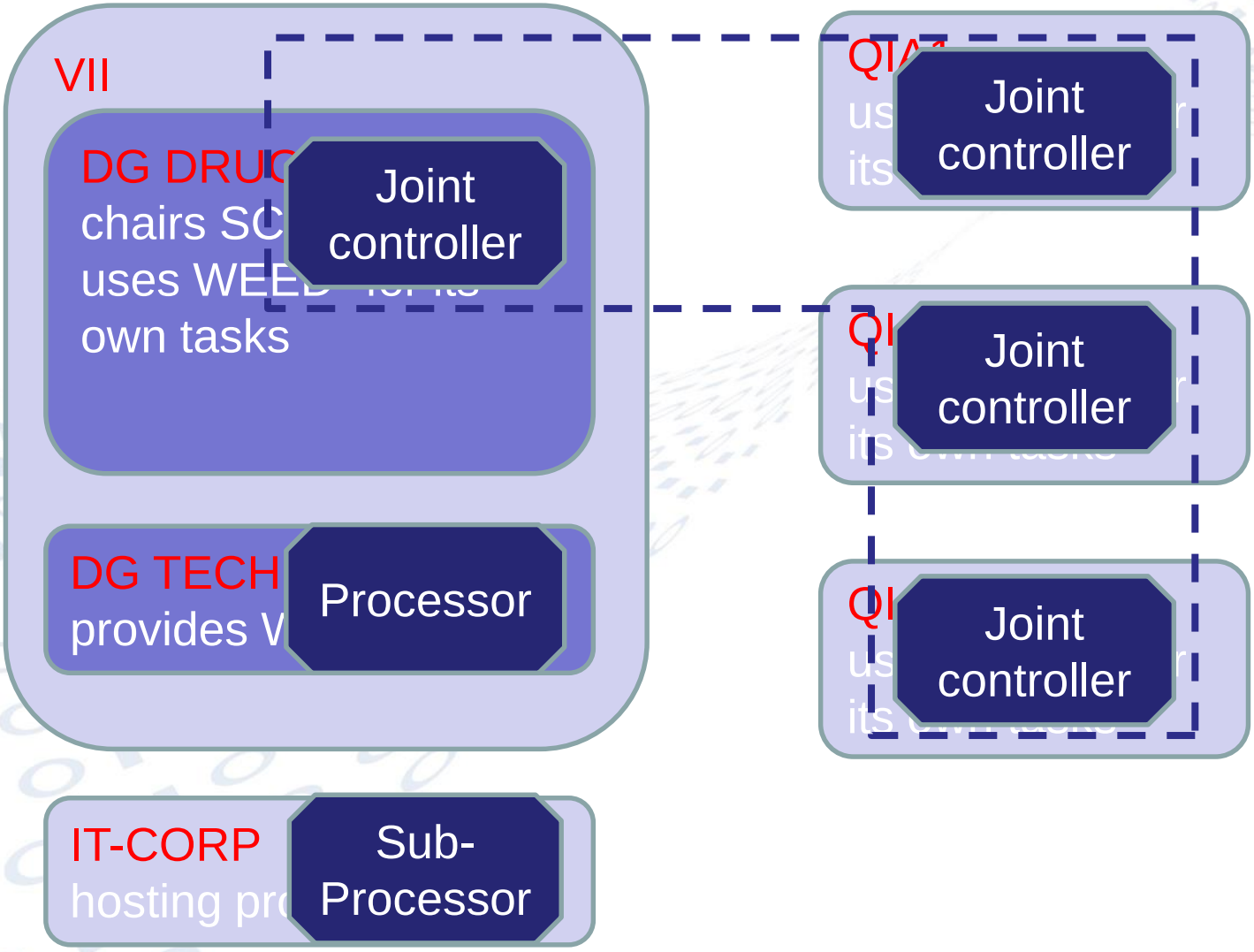
Case study: questions

- Based on the information available, who is (joint) controller, who is processor (for what)?
- What do you think would make sense as a distribution of roles between the different organisations involved for:
  - Informing data subjects?
  - Information security?
  - Data breaches?
  - Managing relations with possible processors?
- What do you think should the arrangement between the joint controllers cover (scope/content)?
- What should be the form of the arrangement?

... and now over to you (30 minutes)!

Questions? Answers!

Who is what?


VII
DG DRU
chairs SC
uses WEE
own tasks
Joint controller
DG TECH
provides V
Processor
IT-CORP
hosting pr
Sub-Processor
QIA
Joint controller
QI
Joint controller
QI
Joint controller

Who does what?

- Informing data subjects?
  - JC that includes data in the system.
- Information security?
  - Each JC responsible for own user management (& authorised use);
  - All JCs jointly define high-level policy and can entrust one JC with lower-level implementation.
- Data breaches?
  - if responsibility is clear, relevant JC takes care of it;
  - cooperation duties, e.g. for investigation.
- Managing relations with possible processors?
  - JCs jointly can decide to assign task of dealing with processor(s) to one of them.

Scope and content of JC arrangement

Possible content of arrangement:

- Governance: how do JCs agree on design / further development?
- Purpose: who does what with the data?
- Interaction with DS
  - who informs?
  - cooperation on replying to e.g. access requests;
  - contact point?
  - Beware of Article 28(3)! (=> put in cooperation duties)
- Data quality: who feeds info, who checks?
- Who keeps which kinds of supporting documentation?

Case study: our answers

Possible content of arrangement (continued):

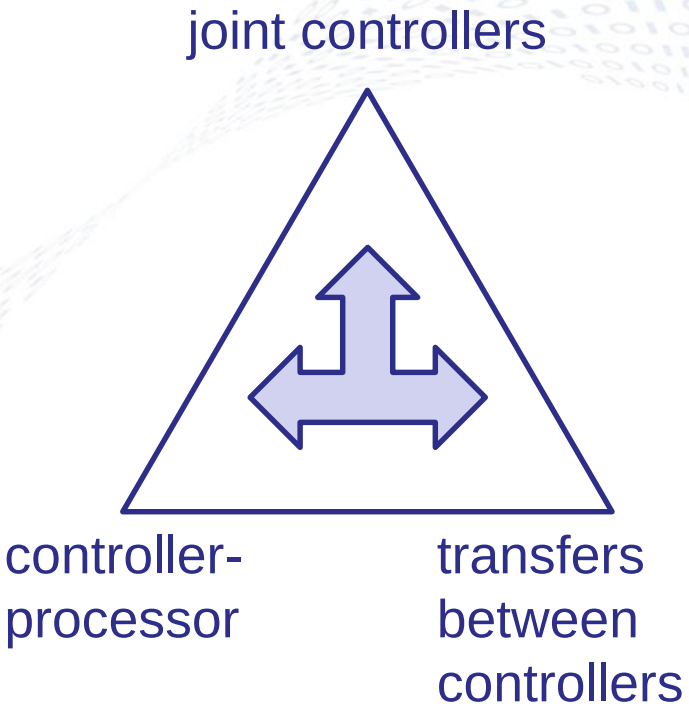
- Security: (common) requirements and responsibilities for implementation, e.g.:
  - user management / access control;
  - logging.
- Cooperation in dealing with compliance obligations (e.g. DPIAs);
- Cooperation in dealing with supervisory authorities, including data breach notifications;
- Use of processors?
- Liability

Case study: our answers

- Form of the arrangement?
  - would usually be some form of MoU;
  - can be supplemented by lower-level SLAs

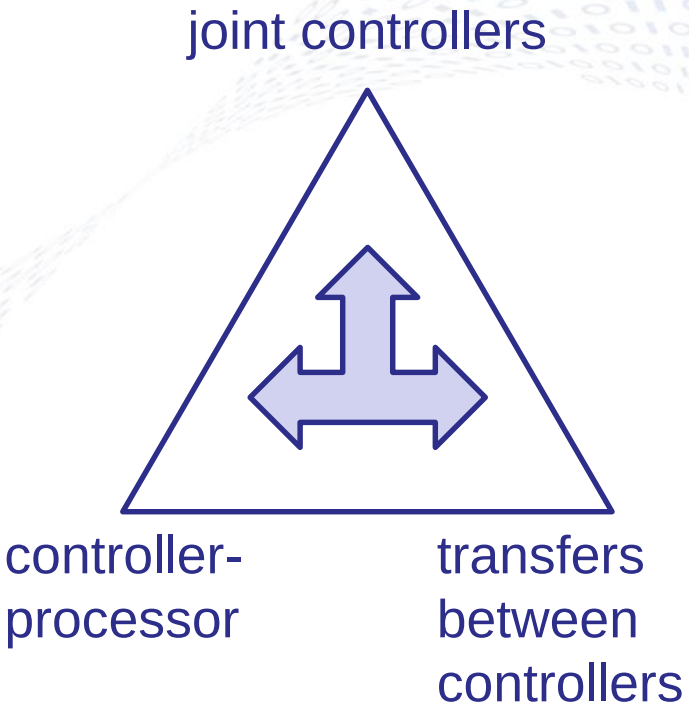
Conclusion

- Joint controllership is not new!
  - ...writing down who does what already was a good idea in the past...
- Not everything is joint controllership
  - ... imagine Europol would receive some reports, possibly including personal data from WEED[2] => transfer (because of different purposes and means)



Conclusion

- Next steps
  - Please provide comments by 06/06/19;
  - EDPS to issue guidelines by 07/2019, including some checklists;
  - EDPB will update its own guidelines.



Thank you for your attention!

For more information:

www.edps.europa.eu
edps@edps.europa.eu

@EU_EDPS