
# Outsourcing: upcoming guidance and case study

**Zsófia Szilvássy**
**Snežana Srdić**

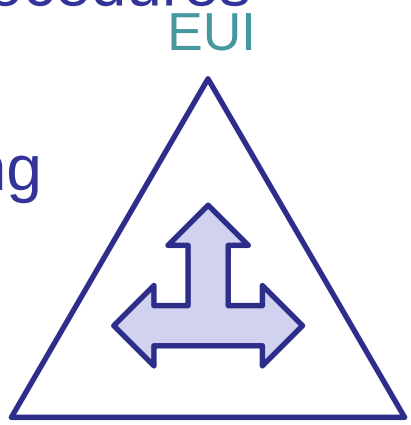
**DPO-EDPS meeting at EIOPA**
**17/05/19**

# Young Zaphod Plays it Safe ... EUIs too

- Upcoming EDPS guidance on outsourcing
- Case study: WEED$^2$ system
- Conclusion

# Upcoming EDPS guidance

- Why?
  - New specific rules in Art. 29
  - general SCCs for processors adopted by EDPS on 07/12/18
  - other SCCs for specific contracts (e.g. IT, external action)
- Scope:
  - update of GLs selection of contractors, grants, experts
  - using standard contractual clauses
  - considerations for procurement/tendering procedures
  - GLs on data protection in outsourcing
  - contracts with processors and sub-processing
  - processing arrangements between EUIs
  - FAQs, example cases, checklists...



# Upcoming EDPS guidance

- Your needs – based on the input from the last DPO meeting:
  - the use of standard contractual clauses with processors
  - the role of the DPO throughout the procedures
  - the selection of contractors and for outsourcing processing operations
  - data protection implications for procurement and for authorising officers

**Feel free to share further needs and above all best practices by 17 June.**

# Upcoming EDPS guidance

- Timeline
  - instructions on use of SCCs for processors adopted by EDPS: sent to you for information in 05/2019
  - other SCCs adopted by EDPS + instructions: 12/2019
  - update of GLs selection of contractors, grants, experts: 12/2019
  - considerations for procurement/tendering procedures
  - EDPS guidelines on outsourcing: 2020
    - contracts with processors and sub-processing
    - processing arrangements between EUIs
  - NB: EDPB guidelines on controller - processor under GDPR EDPS guidelines on joint controllership

# Processor (Art. 29 EUDPR)

- Use only processors providing sufficient guarantees to implement appropriate technical and organisational measures that the processing will meet the requirements of the Regulation and ensure the protection of the rights of the data subjects.
- NOT outsource/subcontract without the prior written authorisation of the controller; keep the controller informed of any changes, giving the opportunity to object;
- Written contract or other legal act with processor with DP clauses
- Pass on same contractual obligations to any subcontractors.
- GDPR compliance one of the elements to demonstrate sufficient guarantees
- Individual DP clauses or SCCs can be used in contracts
- SCCs adopted by EC or by EDPS
- If processor infringes the Regulation by acting as a controller then is considered a controller for that.

# MODEL DATA PROTECTION PROVISIONS

**[SPECIAL CONDITIONS]**

**[I.9.] PROCESSING OF PERSONAL DATA**

**[I.9.1] Processing of personal data by the contracting authority**

For the purpose of Article II.9.1,

(a) the data controller is [*insert position of the data controller and name of the organisational entity*];
(b) the data protection notice is available at https://ec.europa.eu/info/data-protection-public-procurement-procedures_en.

**[I.9.2] Processing of personal data by the contractor**

[This clause is not applicable to this FWC.][1]

[For the purpose of Article II.9.2,

(a) the subject matter and purpose of the processing of personal data by the contractor are [*provide a short and concise description of the subject matter and purpose*];

# 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 own 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 is not able to host the database, so external contractor will need to be hired.
- The SC will define functional and non-functional requirements for WEED$^2$. The system will be built by VII DG TECH, based on instructions from SC.
- IT-CORP, which DG TECH has often used in the past, was selected as a hosting provider for WEED$^2$.
- IT-CORP's has establishments in Norway (data centre), Argentina and Kazakhstan (both helpdesk).

# Case study: WEED²

VII

DG DRUG
chairs SC
uses WEED² for its own tasks

DG TECH
provides WEED²

QIA1
uses WEED² for its own tasks

QIA2
uses WEED² for its own tasks

QIA3
uses WEED² for its own tasks

IT-CORP
hosting provider

Norway data center

Argentina
IT helpdesk

Kazakhstan
IT helpdesk

# Case study: questions

- Will you think of adding specific data protection considerations at the stage of the call for tenders? If yes, which considerations will you think of? In which tendering documents? How?
- What would you include in the contract with IT-CORP? Would you use any standard contractual clauses?
- Do you think that concerns of QIA3 would have an impact on the contract?

- What do you think the arrangement with VII and DG TECH as processor should cover?
- What should be the form of the arrangement?



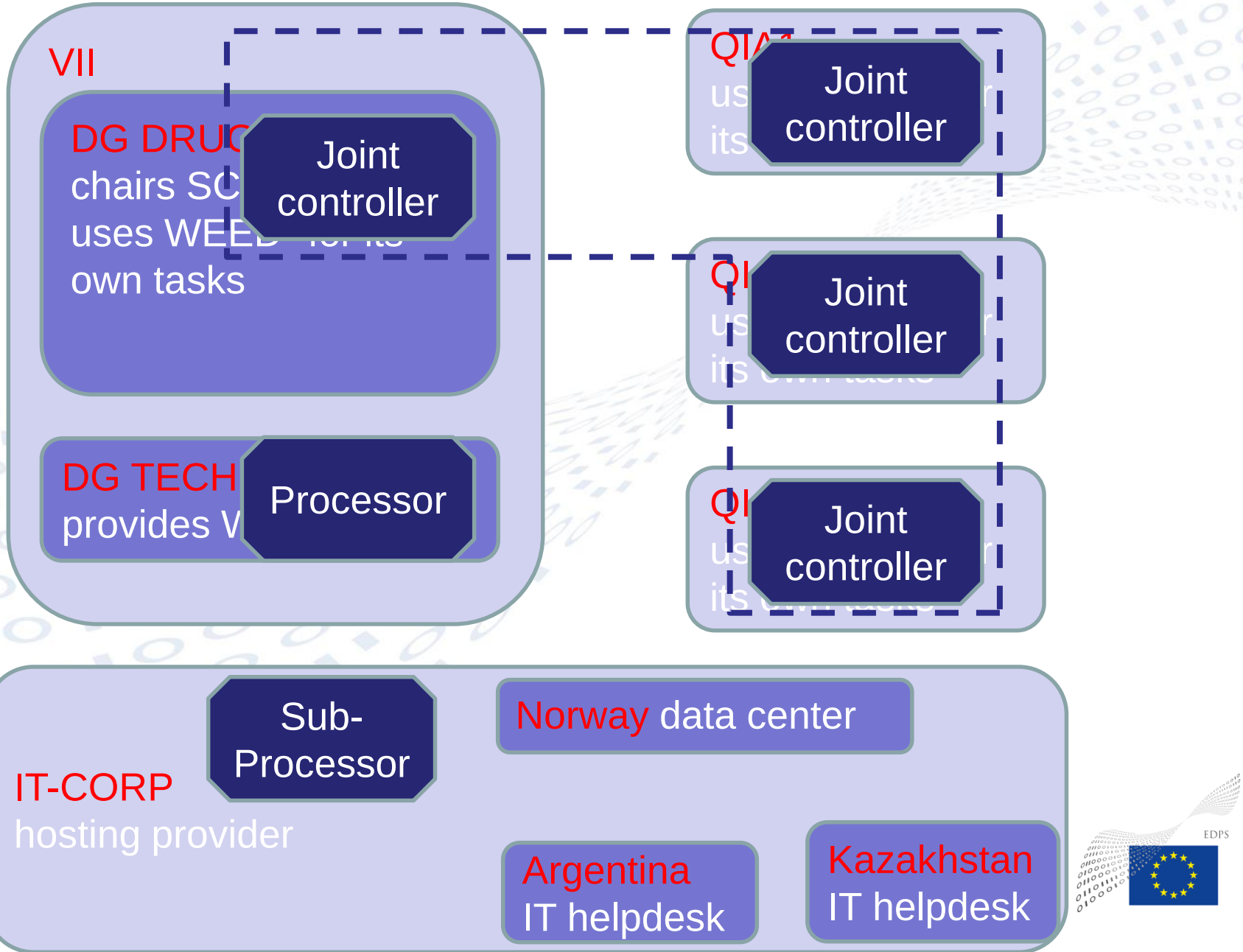
... and now over to you (30 minutes)!

# Questions? Answers!



EDPS

# Who is what?


VII
DG DRUG
chairs SC
uses WEED
own tasks
Joint controller
DG TECH
provides V
Processor
Joint controller
Joint controller
Joint controller
Sub-Processor
IT-CORP
hosting provider
Norway data center
Argentina
IT helpdesk
Kazakhstan
IT helpdesk

# Case study: answers

1) Will you think of adding specific data protection considerations at the stage of the call for tenders?

YES + preliminary risk assessment

If yes, which considerations will you think of?

- *purpose & scope of processing*
- *categories of data & data subjects*
- *retention period*
- *data location & data access*
- *recipients of data and data transfers*
- *security measures*
- *any additional data protection laws (e.g. ePrivacy Directive, NIS Directive)*

*... continued*

# Case study: answers

- *guarantees from tenderers on compliance with d.p. laws*
  - *e.g. GDPR audit reports,*
  - *IT security certifications, IT services management best practices,*
  - *binding corporate rules, standard contractual clauses*
- *explanation from tenderers on how they will follow recommendations in any EDPS' guidelines*
  - *e.g. cloud computing, web applications*

1)

In which tendering documents? How?

- *In technical specifications*
- *As minimum requirements*
- *As selection criteria and/or*
- *As award criteria*

# Case study: answers

2) What would you include in the contract with IT-CORP? Would you use any standard contractual clauses?

3) Do you think that concerns of QIA3 would have an impact on the contract?

- *purpose, duration, nature& scope of processing*
- *categories of data & data subjects*
- *retention period*
- *data location & data access*
- *recipients of data and data transfers*
- *security measures*
- *prohibition of disclosure –reference to the Protocol*
- *any additional data protection laws (e.g. ePrivacy Directive, NIS Directive)*
- *processor may only act upon documented instructions of controller*



*... continued*

# Case study: answers

- *sub-contracting only with prior written authorisation, information on changes*
- *confidentiality, access on a need to know basis*
- *auditing rights and EDPS inspection*
- *division of tasks between joint controllers*
- *assistance with data subject rights requests*
- *assistance with controller obligations (Articles 33-41, records)*
- *assistance with data breaches –set specific deadline*
- *choice to return or delete the data at the end of the processing*
- *obligation to inform the controller if it infringes the Regulation*
- *ground for termination, liability etc.*
- *applicable DP law and other applicable provisions affecting DP, e.g. choice of applicable law, jurisdiction, amendments etc.*

# Case study: answers

3) How far would QIA3 be in a position to check that IT-CORP does its job in the right way?

- *Controllers have the right to audit processors and sub-processors.*
- *Which of the joint controllers would do the audits, depends on the division of tasks between the joint controllers.*
- *The joint controller assigned the task of managing relations with processors and/or the one with best in-house IT capabilities would be best placed to do the audits.*
- *That joint controller should keep other joint controllers fully informed of audits and results and take any of their concerns into account.*

- *In this case, VII would be the logical one.*

# Case study: answers

3) How far could IT-CORP's establishments in Norway (data centre), Argentina and Kazakhstan (both helpdesk) be involved?

- *DG TECH should demonstrate to DG DRUG that it has signed a contract with IT-CORP which passes on same processor obligations that are in SLA between DG DRUG and DG TECH onto IT-CORP for what is subcontracted, including safeguards (e.g. SCCs) for international transfers between processors*

- *GDPR is applicable in Norway as well as Belgium*
- *Argentina is in the COM's list- has adequate level of DP*
- *IT-CORP should demonstrate to VII that technical and organisational safeguards are in place in all IT-CORP subsidiaries and establishments*

  *(e.g. Binding Corporate Rules of IT-CORP are signed and followed, confidentiality commitments, checks and audits by IT-CORP head office)*

*... continued*

# Case study: answers

3) How far could IT-CORP's establishments in Norway (data centre), Argentina and Kazakhstan (both helpdesk) be involved?

- *As to IT-CORP's Kazakhstan establishment, VII should make a risk assessment on its involvement. Can decide:*
  - *not to permit involvement of Kazakhstan establishment*
  - *permit with additional safeguards (e.g.*
    - *BCRs, contract clauses, confidentiality commitments,*
    - *staff vetting, periodic reporting on checks by IT-CORP, additional checks and audits by DG TECH,*
    - *IT security certifications, IT services management best practices).*

# Case study: answers

4) What do you think the arrangement with VII and DG TECH as processor should cover?

5) What should be the form of the arrangement?

- *everything which is in the contract with IT CORP*
- *legally binding act*
  *e.g. MoU with VII, SLA DG DRUG with DG TECH*

# What to sign?

VII

DG DRUG
chairs SC
uses WEED² for its own tasks

SLA

DG TECH
provides WEED²

MoU

QIA1
uses WEED² for its own tasks

QIA2
uses WEED² for its own tasks

QIA3
uses WEED² for its own tasks

Contract

IT-CORP
hosting provider

Norway data center

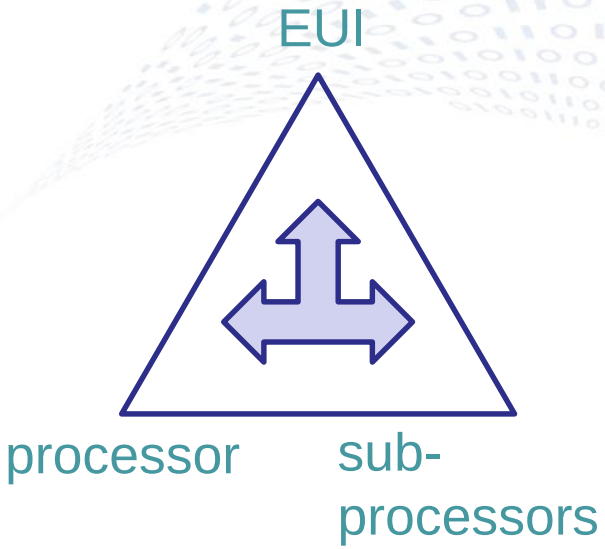
BCRs

Argentina
IT helpdesk

Kazakhstan
IT helpdesk

# Conclusion

- Contracting is not new!
  - ...writing down who does what already was a good idea in the past...
- Keep control, assess risks and carry out audits
- Mind sub-contractors and transfers
  - ... imagine IT-CORP would be obliged to send data from WEED$^2$ to LEA of US => transfer



# Thank you for your attention!

**For more information:**


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

@EU_EDPS