Case study on contracts with IT service providers

Zsófia Szilvássy

DPO-EDPS meeting at Historical Archives of the European Union

7/11/2019

Overview

1. What is outsourcing?
2. Case study
3. Answers

Outsourcing

- **Processing carried out on behalf of the controller**
  e.g.: medical services, external experts, IT services
- **Risk assessment or DPIA** before tendering procedure launched
- **Contract or other legally binding act** governs outsourcings
- **Due diligence before you outsource processing** to avoid any surprises,
  e.g. unknown reuse of your data, unknown subcontractors and transfer of your data to third countries

The actors for contracts with IT service providers

Top management
Accountable

Business owner
Responsible

DPO
Advisor

IT department
Security designer

Processor
Executor

Basic principles

- Accountability
- Privacy by design and by default –think data protection
- Lawfulness
- Purpose limitation
- Data minimisation
- Accurate and where necessary kept up to date
- Keep data no longer than is necessary
- Implement security measures

Outsourcing

Controllers and processors accountable!

« *Procure secure* »

- Minimum requirements, selection or award criteria
- Remember privacy by design & by default

Contract or other binding legal act in place

- Use Standard Contractual Clauses adopted by EDPS (DG BUDG templates) and adapt them their to your needs
- Clarify roles controller/processor
- Contractual safeguards (security, confidentiality, data location)
- Processor should act only on behalf of the controller
- Privacy statements,
- Control sub-sub-contracting and transfers of personal data

Controller can verify compliance via audits

Legal basis - Processor (Art. 29)

- 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 for subcontractors, giving the opportunity to object;

Legal basis - Processor (Art. 29)

- 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 for processors **adopted by EC or by EDPS**
- If **processor** infringes the Regulation by acting as a controller then is **considered as a controller** for that.

Controller & list of Art. 29

The Controller should

- ✓ use only processors providing sufficient guarantees to implement appropriate **technical and organisational security measures**, including localisation of data
- ✓ **allocate** the responsibilities/tasks of the processor,
- ✓ indicate precisely the **subject-matter, duration, nature, purpose** of the processing,
- ✓ determine the **retention period** of personal data and choose whether the processor should delete or return all the personal data to the controller after the end of its service,
- ✓ **can verify whether the processor is in compliance via audits; processor should allow for and contribute to audits/inspections.**

Processor & list of Art. 29

The Processor should

- ✓ process data only on the **documented instructions** from the controller,
- ✓ **assist the controller** with the obligation to guarantee the **rights of data subjects** and to fulfil the controllers obligations pursuant to Articles 33-41 of the Regulation
- ✓ **notify personal data breaches** within 48h to the controller
- ✓ **notify** any legally binding **request for disclosure** of the personal data processed on behalf of the controller and may only give access to data with the prior written authorisation of the controller
- ✓ **NOT process data for other incompatible purposes**
- ✓ **NOT outsource/subcontract**; only with the prior written authorisation of the controller; should inform controller of any changes, giving controller the opportunity to object; pass on same contractual obligations to any subcontractors.

Standard Contractual Clauses adopted by the EDPS

STANDARD CONTRACTUAL CLAUSES FOR DATA PROCESSORS[1]

[I. 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-proc *evant data protection notice*]

Case study

TRICK OR TREAT

Case study: Trick or Treat

- The *Very Important EU Institution* (VII) needs to buy an IT software and optional connected services for its daily operation, to browse internet, redact, collaborate and exchange documents, send e-mails
- VII has an old version of license Zombie, so the new software needs to be compatible to ensure business continuity
- VII receives an offer and a standard license agreement from Trick or Treat Ltd (ToT) for an updated version of Zombie

Case study: Trick or Treat

- ToT is based in the United States, has data centers in Armenia and Germany and a center for helpdesk services in Argentina and Marocco.

- ToT includes in its offer that some data should be collected from users and analyzed in their headquarters and by their subcontractors to ensure optimal services to users.

Case study: questions

1. ToT suggests to sign its own standard license agreement and terms of use. Your legal department is wondering whether the selected terms are in compliance with Regulation 2018/1725. What would you advise as a DPO?

2. What would you include in the contract with ToT?

3. Do you think that the location of the headquarters, data centres and the helpdesk would have an impact on the contract?

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

Questions? Answers!

EDPS

Case study: answers

General practices of IT service providers

Use of intermediaries

- Selected through tendering procedures, sign a Framework Contract (with DP clauses) with the controllers, negotiate price with providers
- License agreements are "negotiated" and signed directly between the service provider and the EUI
- License Agreements are not specific contracts under the FWC

License Agreements

- complex documents, often including a master/main agreement, specific agreements, user terms, product terms, service terms, etc.
- user terms, product terms, service terms and privacy policies are set and changed by the service provider at their discretion
- Normally master agreements prevail - in practice there is no clear order of precedence, rather derogation to subordinated documents
- standard model agreements and user terms and privacy policies set by the service providers
- take it or leave it – difficult to negotiate individually

Case study: answers

1. Assessment of the selected terms of the license agreement

1. Use and collection of and access to service data:

- definition of personal data
- uses of personal data for all reasonable and necessary purposes
- right to use, reproduce, modify, and otherwise exploit the data for the purpose of improving and enhancing
- access to foreign authorities for LE

- **Definition of personal data – link to transfers**
- **Purpose limitation**
- **Inviolability of archives –the EUI shall agree in writing to grant access in a specific request**

Case study: answers

1. Assessment of the selected terms of the license agreement

2. Applicable law

- laws of the State of California –excluding any conflicts of laws
- jurisdiction federal courts of San Francisco, California
- no guarantee for compliance with other laws

- ***Regulation 2018/1725 (+ additional DP laws)***
- ***EU law + law of the Member States where EUI established***
- ***Jurisdiction of the Member State where EUI established***

Case study: answers

1. Assessment of the selected terms of the license agreement

3. Modification of the Agreement

- unilaterally by ToT Ltd –notification to the EUI
- customers responsibility to monitor changes published

- **Modifications agreed by both parties**
- **Cannot deviate from applicable data protection law**

Case study: answers

1. Assessment of the selected terms of the license agreement

4. Limitation of liability

- liability excluded for loss of use, loss of business information, loss of revenue, or interruption of business

➢ ***Watch out! Excludes liability for non-compliance issues, data breaches, fines...***

Case study: answers

1. Assessment of the selected terms of the license agreement

5. Verifying use of license

- ToT Ltd or its auditor can verify compliance with the license terms
- EUI must provide any (!) information, including access to systems

- **Violates Protocol on Immunities and Regulation 2018/1725**
- **Auditing rights for the EUI (EDPS inspection) instead**

Case study: answers

1. Assessment of the selected terms of the license agreement

6. Subcontracting

- ToT Ltd may use subcontractors
- ToT Ltd is free to change the list of subcontractors the contract – obligation to notify the EUI

➢ **Prior written agreement to use or change subcontractors**

➢ **Right to object**

➢ **Comprehensive information to be provided for physical location of the servers used, its sub-processors and locations from where remote operations are performed**

➢ **EUIs must be able to assess risks and verify compliance**

Case study: answers

1. Assessment of the selected terms of the license agreement

7. Transfer of data

- to the U.S. / any other country or to ToT Ltd or its subcontractors under their privacy terms

➢ **All transfers must be done in compliance with Chapter V of the Regulation**

Case study: answers

2. Elements to be included in the contract with ToT

- risk assessment already during the planning of the procurement procedure
- all data protection considerations to be included in the tendering procedure (minimum requirements, selection or award criteria)
- request and verify guarantees from tenderers on compliance with data protection laws

  e.g. GDPR audit reports, IT security certifications, IT services management best practices, binding corporate rules, SCCs
- explanation from tenderers on how they will follow recommendations in any EDPS' guidelines
- **Use SCCs for processors and adapt them to your needs**
- **Use SCCs for international transfers and adapt them**

Case study: answers

2. Elements to be included in the contract with ToT

- 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
- 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. Impact of the location of the headquarters, data centres and the helpdesk

- Controllers have the right to **audit** processors and sub-processors
- Contract in place between ToT and subcontractors **passes on processors the same obligations** that are in the License Agreement with VII (including safeguards for international transfers between processors)
- general principle for data transfers - **equivalent level of protection** for natural persons
- **Chapter V** of Regulation 2018/1725 applies
- in this particular case it can be based on adequacy decisions or on appropriate safeguards
- in all cases the controller should **asses** if the data transfer is necessary and proportionate, what are the risks for people
- **tailored additional safeguards** should be included in the contract, SCCs for processors are not sufficient for transfers

Case study: answers

3. Impact of the location of the headquarters, data centres and the helpdesk

- GDPR is applicable in **Germany**
- **Argentina** is in the COM's list- has adequate level of DP, but the need for additional contractual safeguards should be assessed
- ToT should demonstrate to VII that technical and organisational safeguards are in place in all subsidiaries and establishments
  - (e.g. Binding Corporate Rules of ToT are signed and followed, confidentiality commitments, checks and audits by ToT headquarters)
- Concerning **Armenia** and **Morocco** VII should make a risk assessment on their involvement and can:
  - limit storage of data to Germany or
  - permit the use of the Armenian data center with additional safeguards (e.g. BCRs, contract clauses, confidentiality commitments, trainings, periodic reporting on audits by ToT, additional checks by VII, request IT security certifications)

What can go wrong?

- your data may be processed for further incompatible purposes
- your data will end up in unknown locations, with unknown subcontractors
- security of processing compromised
- onward transfers to further third parties
- unauthorized access – including foreign LEAs
- unilateral amendments – applicable law, substantial conditions change
- foreign law, foreign jurisdiction applicable – not providing for equivalent level of protection for people
- unauthorized access to your premises, access to confidential data

You lose control...

do not cover yourself only for Halloween...

57.10. Acceptable Use; Safety-Critical Systems. Your use of the Lumberyard Materials must comply with the AWS Acceptable Use Policy. The Lumberyard Materials are not intended for use with life-critical or safety-critical systems, such as use in operation of medical equipment, automated transportation systems, autonomous vehicles, aircraft or air traffic control, nuclear facilities, manned spacecraft, or military use in connection with live combat. However, this restriction will not apply in the event of the occurrence (certified by the United States Centers for Disease Control or successor body) of a widespread viral infection transmitted via bites or contact with bodily fluids that causes human corpses to reanimate and seek to consume living human flesh, blood, brain or nerve tissue and is likely to result in the fall of organized civilization.

Add zombies and humour

Thank you for your attention!

For more information:

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

@EU_EDPS