Wojciech Rafał Wiewiórowski

Assistant Supervisor

Brussels, 23 May 2019

**C 2019-0145**

Please use edps@edps.europa.eu for all correspondence

**Subject: Consultation on application of data protection clauses in your contracts**

Dear,

On 14 February you have sent two consultation requests on the use of the Standard Contractual Clauses adopted pursuant to Article 29(8) of Regulation 2018/1725:

1. You have received an enquiry from *contracting authority* *1* on the use options under Article I.9.2., concerning their current contractor, registered in a third country. In your view the territorial clause is restrictive in terms of access to procurement and you are wondering how to ensure that those clauses do not restrict access to the market as provided for in Article 176 of the Financial Regulation. You consider that even if the GDPR is not applicable, Regulation 2018/1725 applies to the processing of personal data in the context of the contract concluded between the contracting authority and the contractor, irrespective of the territory where the data will be processed. You asked the EDPS what would be the options that *contracting authority* *1* should use under Article I.9.2 and whether Article I.9.2 could be removed from the model contract?

2. A second question came from *contracting authority* *2* to clarify whether Regulation 2016/0679 (the GDPR) or Regulation 2018/1725 applies to the processing of personal data of the staff of Contracting Authority 2 by the Contractor. *Contracting Authority* *2* raised the issue of the articulation between the two Regulations in the contract: (i) in Article II.4.3 of the model FWC it is provided that the contractor should comply as minimum requirement with the GDPR; while (ii) Article II.9.2 provides that the processing of personal data by the contractor should meet the requirements of Regulation 2018/1725. In your view, it is Article II.9.2 of the contract which applies to the contractor when it process personal data of the staff of the Controller. In this context you were wondering whether the current Standard Contractual Clauses of the model contracts provide for an adequate protection when it comes to the processing of personal data of the staff of the contracting authority.

***1. The Contracting Authority 1 consultation***

Concerning the question on access to procurement, the intention behind the options offered in points (i) to (v) under I.9.2 is definitely not to restrict competition, but to **protect fundamental rights and freedoms of individuals**. The options proposed in points (i) to (v) do not (and should not) exclude participation of tenderers / contractors established in third countries, but they should provide for appropriate legal and technical safeguards for the processing of personal data to be complied by all tenderers on equal terms. The choice between the options in points (i) to (v) should be made following a **case by case assessment done by the controller** considering likelihood and severity of the risk to the rights and freedoms of people, which should be determined by reference to the nature, scope, context and purposes of the processing.

In line with the principle of accountability, it is for the controller to assess and mitigate the risks. In this context, they need to identify the appropriate legal and technical safeguards to ensure that both the controller and the processor (contractor, and -where relevant- any subcontractors) comply with their obligations deriving from Regulation 2018/1725. Even if the controller concludes that there are risks or high risks to the rights of individuals and concludes that compliance with the Regulation can only be ensured if the data is stored or processed or accessed, only in the territory of certain third countries and the EEA or only within the EU, these conditions do not exclude per se participation of tenderers established in third countries. This is a matter of compliance with EU law (set also as minimum requirements) through legal and technical safeguards to be included in the technical specifications, allowing for participation for all tenderers on equal terms. This means that these safeguards have to be in place whenever data are transferred out of the EU/EEA, whether by a non-EU/EEA-based entity or by an EU/EEA-based entity to a non-EU/EEA-based subcontractor. In addition, many multinational or foreign companies have branches in the EEA and already offer tailored services with data centres in Europe to mitigate eventual risks.

Concerning the **question of *contracting authority* *1***, we confirm that all processing of personal data by the contractor or other contractors carried out on behalf of contracting authority *1* must be done in compliance with Regulation 2018/1725, irrespectively from the place of establishment of the contractor. In the present case, as the controller (EUI) is subject to Regulation 2018/1725, therefore the contractor’s processing operations should meet the requirements of Regulation 2018/1725 as well. For any parts of the processing where the contractor acts not in line with instructions of the EUI, beyond its role as processor for the EUI, The contractor takes on a role of the controller for that processing (see Article 29(10) of Regulation 2018/1725). In that exceptional case, the contractor is subject to the GDPR based on Article 3 of the GDPR since:

* applicants for EUI competitions for officials and temporary or contractual agents are limited to EU citizens, the contractor is providing services to EU citizens or monitoring their behavior and
* moreover, the contractor has establishments in several EU Member states.

Also, please note that all cases where the data is leaving the territory of the EU (including access from a third country) are considered as an international transfer, which has to comply with the conditions set out in Chapter V of Regulation 2018/1725, i.e. equivalent level of protection of personal data must be ensured. This Chapter sets out that personal data may be transferred to third countries based on an adequacy decision of the Commission, or in the absence of that in case  the controller or processor has provided appropriate safeguards (based on legally binding and enforceable instruments between public authorities or bodies; or on standard data protection clauses adopted by the Commission or by the EDPS or based on binding corporate rules, or codes of conduct or certification mechanisms pursuant to the GDPR) or in case the EDPS authorized the transfer /clauses. It should nevertheless be underlined that even if  a third country, in principle, provides for an equivalent level of  protection of personal data for international transfers, the risks to rights and freedoms of individuals should be assessed on a case by case basis, considering the nature, scope, context and purposes of the processing and contractual safeguards should be implemented accordingly. This is also in line with the obligation of the controller set out in Article 29(1) to use only processors providing sufficient guarantees to implement appropriate technical and organisational measures that the processing will meet the requirements of Regulation 2018/1725 and ensure the protection of the rights of the data subjects.

As concerns the processing carried out by *contracting authority* *1*, the controller should carefully assess the risks to right and freedoms of individuals. We draw your attention to Recital 45 of Regulation 2018/1725, setting out some examples of risks, including in particular cases: where personal data are processed which reveal racial or ethnic origin, the processing of data concerning health; **where personal aspects are evaluated**, in particular analysing or predicting aspects concerning performance at work, reliability or behavior; or where processing involves a large amount of personal data and affects a large number of data subjects. Based on the available information, we are not in a position to advise the contracting authority on the content of the contract or of the technical specifications to be published.

In any case, please note that **Article I.9.2 can only be deleted for contracts where processing of personal data is not outsourced** at all. In order to be in compliance with Regulation 2018/1725, Article I.9.2 (a) must set out the subject matter and the purpose of the processing operation, while Article I.9.2. (b) (i)-(iii) should also be adapted with care for all processing operations (indicating the countries where the personal data at stake can be processed, stored, accessed). In any case, Article I.9.2 (b)(iv) remains applicable. Concerning Article I.9.2 (b)(v) it may be worth to clarify in the vademecum, that it is without prejudice to the provisions set out in points (i)-(iii), i.e. in case  a controller made the choice to store or process data only in the EU or the EEA no international transfers can take place.

***2. Contracting authority 2 consultation***

Concerning ***contracting authority* *2*’s question** we agree with your interpretation, the contractor shall ensure that the processing of personal data on behalf of an EU institution is carried out in compliance with Regulation 2018/1725 in line with Articles I.9.2 and II.9.2.

Should you have any further questions, please do not hesitate to get back to us. We look forward to receiving the documentation from *contracting authority 1* for a more detailed analysis.

Best regards,

Yours sincerely,

[signed]

[Wojciech Rafał WIEWIÓROWSKI](http://www.giodo.gov.pl/1520097/j/pl/)

Cc: (DPO)