JHS 166 Terms and Conditions of Public IT Procurement

Annex 9. Special Terms and Conditions for the Processing of Personal Data (JIT 2015 – Personal Data)

Version: 1.0
Published: 25 June 2018
Validity: until further notice

INSTRUCTIONS FOR USE

These Special Terms and Conditions are intended to be used in situations where the supplier processes personal data on behalf of the client as part of a procured service. These terms and conditions are not intended to be used on their own; instead, the Special Terms and Conditions applicable for each service and the Terms and Conditions of Public IT Procurement (*JIT 2015 – General Terms and Conditions)* should also always be appended to the agreement. It is recommended that these terms and conditions be adopted before the other Special Terms and Condition in the order of application of appendices.

If necessary, the agreement should determine the 'controller' and 'processor' and to take into account the requirements set in the EU's General Data Protection Regulation *(EU) 2016/679* for the processing of personal data. The client shall be the controller as referred to in legislation concerning the processing of personal data and data protection when it determines the purpose and practices for processing personal data. Although the client is typically the controller of the personal data related to the service, it is worth noting that the supplier may also possess personal data related to its activities which it may utilise in the service. These include contact information recorded in the supplier's customer register. The client's instructions do not cover such data.

It is recommended that a document concretely specifying the subject-matter, nature and purpose of the processing of personal data be appended to the agreement. According to Article 28 of the *EU's General Data Protection Regulation,* the processing of personal data shall be governed by a binding document that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects.

The contracting parties shall determine the level of security required for the service which is the object of the agreement in collaboration. The required level of security may be based on, for example, risk assessment carried out by the client and discussed together between the parties, available technology and technological opportunities as well as the nature and quality of the processed data.

According to the General Data Protection Regulation, the controller must approve of the subcontractors used by the controller with prior authorisation. The issued prior written authorisation may be specific or general. In addition, the supplier shall inform the client of any planned changes concerning subcontracting. The client may give written authorisation for use by subcontractor processors by signing an agreement specifying the used subcontractors, for instance.

JIT 2015 – General Terms and Conditions lays down provisions on compensation for damage and possible right of subrogation between the controller and processor.

These use instructions do not form part of the agreement.

Contents

1 Scope of application

(1) These Special Terms and Conditions are applied to the procurement of services which involve the processing of personal data by the supplier by public procurement units, if these terms and conditions are referred to in the agreement and to the extent it has not been otherwise agreed in writing.

(2) These Special Terms and Conditions are used together with the General Terms and Conditions of Public IT Procurement. In case of any conflict, these Special Terms and Conditions take precedence over the aforementioned General Terms and Conditions of Government IT Procurement with regard to their corresponding provisions.

2 Definitions

In addition to the following definitions of the Special Terms and Conditions, the definitions of *JIT 2015 General Terms and Conditions* shall be applied.

processor
fi käsittelijä

a party referred to in personal data legislation which processes personal data on behalf of the controller

controller
fi rekisterinpitäjä

a party referred to in personal data legislation which, alone or jointly with others, determines the purposes and means of the processing of personal data

personal data legislation
fi tietosuojalainsäädäntö

the General Data Protection Regulation of the European Union (EU) 679/2016 as well as other statutes on data protection and provisions by the data protection authorities

personal data breach
fi henkilötietojen tietoturvaloukkaus

a data breach leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed

the client's personal data
fi tilaajan henkilötieto

any personal data the client is responsible for as the controller

3 The roles of the contracting parties in processing personal data

(1) The client shall act as the controller and the supplier as the processor, unless otherwise agreed or stipulated by the purpose of the processing of personal data. The agreement shall specify the tasks and responsibilities of the contracting parties related to the processing of personal data in further detail.

(2) The subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, applicable data security measures, and more detailed obligations and rights of the supplier and client shall be described more specifically in the agreement, its appendices or the client's instructions. The supplier shall comply with the terms and conditions laid down in the agreement, its appendices and related instructions.

4 General obligations of the supplier

(1) The supplier shall comply with the processing practice required under the effective legislation on data protection and with any provisions on the processing and protection of personal data. The supplier shall ensure that the service complies with the valid legislation on data protection and the requirements of the agreement, paying particular attention to the provisions on data protection by design and by default.

(2) The supplier shall take the appropriate technical and organisational measures to ensure that the processing of the client's personal data is implemented in accordance with the requirements of the agreement and the agreed practices. The purpose of these measures is to ensure the lawful processing of personal data as well as the confidentiality, integrity, availability and resilience of the systems used for processing personal data.

(3) The supplier may not process or otherwise utilise the personal data it processes on the basis of the agreement for purposes and extent other than the purposes of the agreement.

(4) The supplier shall appoint a data protection officer or a contact person in charge of data protection for contacting related to the client's personal data. The supplier shall provide the client with the contact information of the data protection officer or contact person in writing.

(5) The supplier shall, upon the client's request, make available to the client all information necessary to demonstrate compliance with the obligations laid down for controllers and processors and, upon request, contribute to preparing and maintaining descriptions and other documents, such as impact assessments, for which the client is responsible as well as the implementation of prior consultation in accordance with the General Data Protection Regulation. The supplier shall carry out these tasks with the prices stated in the agreement, unless otherwise agreed.

(6) The supplier shall, without delay, inform the client of all requests by data subjects concerning the exercise of the data subject's rights. The supplier may not respond to these requests. The supplier shall assist the client in fulfilling its obligation to respond to these requests. The requests may require the supplier to, for instance, assist the client in providing information and communicating to data subjects, implementing the right of access of data subjects, rectifying or deleting personal data, imposing restrictions to processing or transferring the personal data of a data subject from one system to another. Unless otherwise agreed, the supplier shall be entitled to invoice the client based on the prices set in the agreement if providing assistance causes additional expenses to the supplier. The supplier is obligated to notify the client in advance of any additional costs to be incurred.

(7) The supplier shall allow for and contribute to inspections conducted by the client or another auditor mandated by the client. More detailed terms and conditions of the inspection procedure are included in the Terms and Conditions of Public IT Procurement (JIT 2015 – General Terms and Conditions) and the agreement.

5 The client's instructions

(1) In the processing of the client's personal data, the supplier shall comply with the terms and conditions agreed in the agreement and these Special Terms and Conditions as well as the written instructions of the client. The client shall ensure that the instructions are maintained and available. The supplier shall inform the client without undue delay if the instructions provided by the client are insufficient or if the supplier suspects that they are unlawful.

(2) The client shall have the right to modify, supplement and update the instructions it has given to the supplier on the processing of personal data and data protection. If the modifications to the instructions cause other than minor changes to the services provided under the agreement, their effects shall be agreed on through the change management procedure in accordance with the agreement.

6 Service personnel

(1) The supplier shall ensure that any person acting under its authority who has the right to process the client's personal data is committed to complying with the confidentiality provisions under the agreement or are bound by the statutory confidentiality obligation.

(2) The supplier shall ensure that any person acting under its authority who has access to the client's personal data is aware of his or her obligations concerning the processing of personal data and only processes the data in accordance with the agreement, these Special Terms and Conditions as well as the client's instructions.

7 Subcontractors processing personal data

(1) If a subcontractor of the supplier processes the client's personal data, the use of the subcontractor requires a prior written authorisation given by the client.

(2) The supplier shall conclude a written agreement with the subcontractor which binds the subcontractor used by the supplier, for its part, to comply with the obligations laid down for the supplier in the agreement as well as the valid instructions on the processing of personal data of the client. The supplier shall ensure that the auditing right under the agreement may also be extended to the subcontractor.

(3) The supplier shall be similarly responsible for the contributions of its subcontractors as it is for its own work. The supplier shall be responsible for ensuring that their subcontractors follow the obligations set for the processor.

(4) The client must be notified in advance of a change to the subcontractor participating in the processing of personal data. The notification must describe how the subcontractor will be processing the client's personal data in accordance with legislation of data protection. The client shall have the right to object a proposed subcontractor for a justified reason.

8 Location of service

(1) Unless otherwise agreed on the location of the service production, the supplier shall have the right to process the personal data of the client in the European Economic Area only. What has been agreed in the agreement and these Special Terms and Conditions shall also apply to the granting of access to the client's personal data via a remote or monitoring connection, for instance.

(2) If the contracting parties agree that the supplier may transfer the client's personal data outside the European Economic Area, the contracting parties shall ensure that the transfer of personal data is implemented in accordance with legislation.

9 Data breaches

(1) The supplier shall notify the client in writing and without undue delay after becoming aware of a data breach concerning the client's personal data regardless of the agreed service hours. In addition, the supplier shall notify the client without undue delay of any other significant disruptions or problems in the service which may affect the status and rights of data subject.

(2) The supplier shall provide the client with at least the following information on the data breach in writing:

i. a description of the nature of the personal data breach, including the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

ii. the name and contact details of the data protection officer or other contact point where more information can be obtained;

iii. a description of the likely consequences of the personal data breach; and

iv. a description of the measures taken or proposed to be taken by the supplier to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

(3) After detecting the personal data breach, the supplier shall immediately take the measures agreed upon in the agreement to eliminate the data breach, and limit and remedy its impacts.

10 Termination of the processing of personal data

(1) During the period of validity of the agreement, the supplier may not delete any personal data it processes on behalf of the client without the explicit request of the client.

(2) Upon the termination or cancellation of the agreement, the supplier shall return to the client all personal data processed on behalf of the client and, at its own expense, destroy any copies of the personal data from its volumes, unless otherwise agreed. The data may not be removed if legislation or an order by the authorities requires for the supplier to retain the personal data. The supplier is not entitled to any separate charge for the delivery of the client's personal data in accordance with this section, unless otherwise agreed.