

## Annex 7. Data protection agreement

### ANNEX 1 to the FRAMEWORK CONTRACT FOR SERVICES

REFERENCE: BSGEE 2023 014

#### Data Processing Agreement

The [Secretary General of the Office of the Secretary General of the European Schools (the 'OSGES') (hereinafter, the 'Controller' of the OSGES) with respect to the processing of the OSGES's personal data], and the [Director of the European Schools of [Brussels I, Brussels II, Brussels III, Brussels IV and Mol (hereinafter, the 'Schools')]] with respect to the processing of the Schools' personal data] (hereinafter all collectively the "controller"),

On the one hand,

AND

[Full official name]

[Official legal form]

[Legal registration number or identity card or passport number]

[Full official address]

[VAT registration number]

(hereinafter, the "subcontractor")

On the other hand,

#### I. Object

The object of these clauses is to define the conditions in which the processor shall undertake to carry out, on behalf of the controller, the personal data processing operations defined below.

Within the framework of their contractual relations, the parties shall undertake to comply with the applicable data protection regulation and, in particular, with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the

processing of personal data and on the free movement of such data (hereinafter referred to as 'the General Data Protection Regulation').

For the purposes of this Data Processing Agreement, terms such as "processing", "personal data", "data controller" and "processor" have the meaning ascribed to them in Article 4 of the General Data Protection Regulation.

If a conflict between this agreement and any other agreement in force between the parties should arise, the terms of this agreement shall prevail.

## II. Description of the processing

The controller determines the scope, purposes and manner in which personal data may be processed by the processor.

The processor is hereby authorised to process on behalf of the controller the personal data required to provide the following service or services [...].

The nature of the operations carried out on the data is [...].

The purpose or purposes of the processing is/are [...].

For performance of the service that is the subject matter of this contract, the controller shall make available to the processor the following necessary information [...]:

- The personal data processed are [...].
- The categories of data subjects are [...].

## III. Duration of the contract

This contract shall enter into force with effect from [...] for a period of [...].

## IV. Obligations of the processor vis-à-vis the controller

The processor shall undertake to:

- **Process the data solely for the purpose or purposes alone that is/are the object of the processing,**
- Process the data in accordance with the controller's instructions appearing in (...) of this contract,
- Inform the controller immediately if it is considered that an instruction constitutes an infringement of the General Data Protection Regulation or of any other provision of Union law or the law of the member states on data protection,
- Inform the controller if the processor is required to transfer data to a third country or to an international organisation, pursuant to the law of the Union or to the law of the member state to which the processor is subject, unless the concerned law prohibits such information on important public interest grounds,
- Guarantee the confidentiality of the personal data processed under this contract,
- Ensure that the persons authorised to process personal data pursuant to this contract:
  - Have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality,
  - Receive appropriate personal data protection training,
  - Take into account, in the case of the processor's tools, products, applications or services, the principles of data protection by design and data protection by default.

The processor may not use the services of another processor to conduct specific processing activities without the prior written authorisation of the controller.

In the event of authorisation, the other processor shall be required to fulfil the obligations of this contract on behalf of and in accordance with the instructions of the controller. It is the responsibility of the initial processor to ensure that the other processor provides the same sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the General Data Protection Regulation. Where the other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.

## **V. Localisation and access to personal data**

Localisation of and access to the personal data processed by the contractor shall comply with the following:

- The personal data shall only be processed within the territory of the European Union and the European Economic Area and will not leave that territory;
- The data shall only be held in data centres located with the territory of the European Union and the European Economic Area;
- No access shall be given to such data outside of the European Union and the European Economic Area;
- The contractor may not change the location of data processing without the prior written authorisation of the contracting authority;

## **VI. Rights of data subjects**

- Obligations of the controller vis-à-vis the processor:

The processor or any other person whose personal data are processed by the controller under these specifications shall have specific rights as a data subject pursuant to Regulation (EU) 2016/679, and in particular the right to access to and rectification or erasure of personal data, the right to restrict processing of those data or, where applicable, to object to it, or the right to data portability.

For all issues concerning the processing of his or her personal data, the contractor or any other data subject whose personal data are processed under these specifications shall approach the controller. He or she may also approach the data protection officer reporting to the controller. Data subjects shall have the right to lodge a complaint at any time with the Belgian Data Protection Authority.

Detailed information about personal data processing may be requested of the controller.

- Obligations of the processor vis-à-vis the controller

The processor shall assist the controller in fulfilment of the controller's obligation to respond to requests for exercising their rights from data subjects whose personal data are processed under these specifications, as provided for in Regulation (EU) 2016/679. The processor must inform the controller of such requests without delay.

## **VII. Notification of personal data breaches**

The processor shall notify the controller of any personal data breach without undue delay and not later than 48 hours after having become aware of it. In this case, the processor shall communicate at least the following information to the controller:

- a) The nature of the personal data breach, including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
- b) The likely consequences of the breach;
- c) The measures taken or proposed to be taken to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and in so far as, it is not possible to provide all this information at the same time, the information may be provided in phases without undue further delay.

After the controller's agreement has been sought and given, the processor shall, in the name of and on behalf of the controller, communicate the personal data breach to the data subject without undue delay, when this breach is likely to result in a high risk to the rights and freedoms of a natural person.

The processor shall assist the controller in complying with the latter's obligations pursuant to articles 31 to 39 of Regulation (EU) 2016/679, namely:

- a) to ensure compliance with the latter's data protection obligations with respect to the security of processing and the confidentiality of personal data;
- b) to notify the Belgian Data Protection Authority of any personal data breach;
- c) to carry out impact assessments relating to data protection and prior consultations to the extent necessary.

## **VIII. Security measures**

The processor must take appropriate technical and organisational measures, having regard to the risks inherent in processing and to the nature, scope, context and purposes of the processing, offering, in particular, as required:

- (a) Pseudonymisation and encryption of personal data;
- (b) The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- (c) The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- (d) A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing;
- (e) Measures designed to protect personal data from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

## **IX. Storage of data**

The duration of processing of personal data by the processor will not exceed the period indicated in [...].

At the end of that period, the contractor must, according to the controller's choice, return, without undue delay and in a jointly agreed format, all the personal data processed on behalf of the controller and copies of those data, or destroy effectively all the personal data, unless Union law or national law requires them to be retained for longer.

## **X. Register of categories of processing activities**

The processor shall maintain a record of all the data processing activities carried out on behalf of the controller, of personal data transfers, of security breaches and of the action taken on requests submitted by data subjects whose personal data have been processed, with a view to exercising their rights, and of requests for access to personal data submitted by third parties.

#### **XI. Disclosure of data by the processor pursuant to a legal obligation**

The processor shall inform the controller without delay of any legally binding request for disclosure of personal data processed on behalf of the controller that is sent to the processor by a national public authority, including an authority in a third country.

The processor shall not be authorised to grant such access without the prior written authorisation of the controller.

#### **XII. Documentation**

The processor shall make available to the controller all information necessary to demonstrate compliance with all the processor's obligations and to allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.