# Annex B - Data protection Standard Contractual Clauses (controller to processor)



## SECTION I

### CLAUSE 1 PURPOSE AND SCOPE

(a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with Article 28(3) and (4) of 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, and repealing Directive 95/46/EC (General Data Protection Regulation).

(b) The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29(3) and (4) of Regulation (EU) 2018/1725.

(c) These Clauses apply to the processing of personal data as specified in Annex II.

(d) Annexes I to IV are an integral part of the Clauses.

(e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 or [for GH being a EC/EU only] Regulation (EU) 2018/1725.

### CLAUSE 2 INVARIABILITY OF THE CLAUSES

(a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.

(b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

## CLAUSE 3 INTERPRETATION

(a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or [for GH being a EC/EU only] Regulation (EU) 2018/1725 respectively, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679 or [for GH being a EC/EU only] Regulation (EU) 2018/1725 respectively.

(c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 OR [for GH being a EC/EU only] Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

## CLAUSE 4 HIERARCHY

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties existing at the time when these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

## CLAUSE 5 - OPTIONAL DOCKING CLAUSE

Not applicable

# SECTION II OBLIGATIONS OF THE PARTIES

## CLAUSE 6 DESCRIPTION OF PROCESSING(S)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

## CLAUSE 7 OBLIGATIONS OF THE PARTIES

### 7.1. Instructions

(a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.

(b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions.

### 7.2. Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

### 7.3. Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in Annex II.

### 7.4. Security of processing

(a) The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

(b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

### 7.5. Sensitive data

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

### 7.6. Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.

(c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or [for GH being a EC/EU only] Regulation (EU) 2018/1725. At the controller's request, the processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.

(d) The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

### 7.7. Use of sub-processors

#### Not applicable

(a) The processor shall not subcontract any of its processing operations performed on behalf of the controller in accordance with these Clauses to a sub-processor, without the controller's prior specific written authorisation. The processor shall submit the request for specific authorisation at least 3 months prior to the engagement of the sub-processor in question, together with the information necessary to

enable the controller to decide on the authorisation. The list of sub-processors authorised by the controller can be found in Annex IV. The Parties shall keep Annex IV up to date.

(b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 and/or [for GH being a EC/EU only] Regulation (EU) 2018/1725.

(c) At the controller's request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.

(d) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the subprocessor to fulfil its contractual obligations.

(e) The processor shall agree a third party beneficiary clause with the sub-processor whereby - in the event the processor has factually disappeared, ceased to exist in law or has become insolvent - the controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

### 7.8. International transfers

(a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or [for GH being a EC/EU only] Regulation (EU) 2018/1725.

(b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

## CLAUSE 8 ASSISTANCE TO THE CONTROLLER

(a) The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.

(b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions

(c) In addition to the processor's obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:

> (1) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

(2) the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;

(3) the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

(4) the obligations in Article 32 of Regulation (EU) 2016/679/ [for GH being a EC/EU only] Articles 33 and 36 to 38 of Regulation (EU) 2018/1725.

(d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

## CLAUSE 9 NOTIFICATION OF PERSONAL DATA BREACH

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 of Regulation (EU) 2016/679 or [for GH being a EC/EU only] under Articles 34 and 35 of Regulation (EU) 2018/1725, where applicable, taking into account the nature of processing and the information available to the processor.

### 9.1 Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

(a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

(b) in obtaining the following information which, pursuant to Article 33(3) of Regulation (EU) 2016/679/ [for GH being a EC/EU only] Article 34(3) of Regulation (EU) 2018/1725, shall be stated in the controller's notification, and must at least include:

(1) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(2) the likely consequences of the personal data breach;

(3) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects. Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(c) in complying, pursuant to Article 34 of Regulation (EU) 2016/679 / [for GH being a EC/EU only] Article 35 of Regulation (EU) 2018/1725, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

### 9.2 Data breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

(a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

(b) the details of a contact point where more information concerning the personal data breach can be obtained;

(c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects. Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay. The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Articles 33 and 34 of Regulation (EU) 2016/679 / [for GH being a EC/EU only] Articles 34 and 35 of Regulation (EU) 2018/1725.

## SECTION III FINAL PROVISIONS

### CLAUSE 10 NON-COMPLIANCE WITH THE CLAUSES AND TERMINATION

(a) Without prejudice to any provisions of Regulation (EU) 2016/679 and/or [for GH being a EC/EU only] Regulation (EU) 2018/1725, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.

(b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

(1) the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;

(2) the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679 and/or [for GH being a EC/EU only] Regulation (EU) 2018/1725;

(3) the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679 and/or [for GH being a EC/EU only] Regulation (EU) 2018/1725.

(c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.

(d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

## ANNEX I

## LIST OF PARTIES

Controller(s):

Name: **The COST Association**, an international not-for-profit organisation (AISBL) under Belgian law, registration number 0829.090.573, represented by Dr Ronald de Bruin, Director of the COST Association, hereinafter referred to as the "**COST Association**",

Address: Avenue du Boulevard - Bolwerklaan 21, 1210 Brussels, Belgium. . . . . .

Contact person's name, position and contact details: .

For practical implementation: Science Administration, science.administration@cost.eu. .

Data Protection Officer: NAME, privacy@cost.eu . . . . . .

Activities relevant to the data transferred under these Clauses: Financing mobility of researchers and innovators in Europe

2. Processor(s):

Name: . . Institution. . . . . .

Address: . . . Full address . . . . .

Contact person's name, position and contact details: . . . . Grant Holder contact point as per article 22 . . . . . .

Activities relevant to the data transferred under these Clauses: Financial, Scientific and Administrative Coordination of COST Action NUMBER. . . . . .

## ANNEX II - DESCRIPTION OF THE PROCESSING

**Categories of data subjects whose personal data is processed**

Working Group participants, MC Members and Observers and any reimbursed participant to an activity of the COST Action NUMBER

**Categories of personal data processed**

| | |
|---|---|
| **Identification data** | |
| Personal identification data | Title, name, first name, private address, phone numbers, email addresses (personal or professional at your choice). |
| **Financial data** | |
| Financial identification data | Bank account numbers, expenses and supporting documents. |
| **Personal characteristics** | |
| Personal details | Age, gender, year and place of birth, citizenship. |
| **Training and studies data** | |
| Academic background and professional qualification | Degree level, PhD thema, year of start of PhD thesis, date of award of PhD, participation in COST trainings. |
| **Professional data** | |
| Professional identification data | Position, institution of affiliation (name and address), place of work, scientific field of expertise, research area. |
| Career | Participation and role in COST Actions, your grants (dates, funding agency(ies)), CV, ORCID id, professional webpage if any |

Sensitive data processed (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures

Not applicable

**Nature of the processing**

unlikely to encounter high risk for the data subject

**Purpose(s) for which the personal data is processed on behalf of the controller**

Implementation of the Financial, Scientific and Administrative Coordination (FSAC) of the Action as described in the Annotated Rules for COST Actions.

**Duration of the processing.**

Duration of the Grant Agreement + extended retention period due to Article 8 of the Action Grant Agreement- Record keeping obligations

**For processing by (sub-) processors, also specify subject matter, nature and duration of the processing**

Not applicable

## ANNEX III

## TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

e-COST is developed and maintained with security of data as a key principle. Refer to e-COST Privacy Notice for overall information on data privacy.

e-COST platform is using AWS (Amazon Web Services) as provider, it is running on redundant infrastructure deployed over different availability zones ensuring high availability. Physical access to infrastructure is not allowed and all e-COST data are encrypted so that any physical access to server / database does not grant access to the data. More advanced details can be found on AWS Privacy Notice.

Use of e-COST requires user to be registered, the registration is based on unique email address of the user that must be functioning for the account to be activated. Access to e-COST is then granted through a login process secured by a password with requirements (minimum 10 characters including variations of case and type: letters, numeric, special characters). The password recovery process requires access to the email address used at registration. Personal data of the user are managed through the profile menu and they can be updated at any time by the user. Important changes on user profile or important actions in account trigger a notification to all email addresses of the user in order to detect potential issues.

COST Association personnel has higher requirements for login to e-COST by the mean of SSO (Single Sign-On) associated to the office environment, itself benefiting from 2-factor authentication, audit logs and monitoring.

Standard user profiles in e-COST do not get access to data beyond what is displayed publicly on COST website.

Grant Holder roles of COST Actions have access to personal data of users needed for the management of the Action and in particular payments to be made (e.g. access to bank details for reimbursing expenses or paying grants).

COST Association personnel has privileged access to user profiles and related personal data; that justifies the higher requirements on account security.

Secured communication channels are established for transmission of e-COST data (including some personal data) to following third party platforms: COST website, e-Signature provider, COST accounting software.

For security and technical purposes, access logs (IP address, visited pages, user agents) are collected for 14 days and stored in logging system of AWS. All actions taken in e-COST are recorded in audit logs with a retention period of 12 months. Logs are only available for e-COST IT administrators through AWS

The e-COST development team is following security best practices to maintain and adapt e-COST to the needs of COST Association, using state-of-the-art tools and monitoring carefully daily functioning. Whenever a potential security threat is detected or brought to its knowledge, the threat is evaluated immediately and handled with the priority required based on the assessed risk.

## ANNEX IV

## LIST OF SUB-PROCESSORS

Not applicable