



Education, Audiovisual and Culture Executive Agency

RECORD OF PERSONAL DATA PROCESSING

Art. 31 REGULATION (EU) 2018/1725 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (henceforth the "Regulation")

Record n°

6/2019

(N° provided by the Data Protection Officer)

In accordance with Article 31(1) of Regulation 2018/1725, individuals whose personal data are processed by the Executive Agency in any context whatsoever are to be protected with regard to the processing of personal data and the Executive Agency has to keep records of their processing operations.

This record covers two aspects:

- 1. Mandatory records under Art 31(1) of the Regulation (recommendation: make the header and part 1 publicly available)*
- 2. Compliance check and risk screening (initial; part 2 is internal only to the Agency, not published)*

The ground for the record is (tick the relevant one):

- ☒ *Regularization of a data processing operation already carried out*
- ☐ *Record of a new data processing operation prior to its implementation*
- ☐ *Change of a data processing operation.*

[Title of the processing operation] (this part may be public)	
1	Last update of this record (where applicable) August 2018
2	Short description of the processing Erasmus + Virtual exchange is a project to promote intercultural dialogue and improve the skills of young people through digital learning tools. Activities will take place as part of higher education programmes or organised youth projects, and will also be offered to individuals who meet the eligibility criteria.

	All information related to the Erasmus+ Virtual Exchange initiative and links to the distinct project activities are gathered on a Hub, hosted on the Youth Portal. This Hub connects potential users to online platforms hosted on external websites offering different types of virtual exchange activities.
3	Approval of controller
	[name]
Part 1 - Article 31 Record (This part may be public)	
4	Name of the Controller Unit(s) and/or function of person acting on behalf of the Controller
	<p>The European Commission represented by the Directorate-General for Education, Youth, Sport and Culture (DG EAC) on the one hand, and the Education, Audiovisual and Culture Executive Agency (EACEA) on the other hand, are joint controllers.</p> <p>Person designated as being in charge of the processing operation: Head of Unit A5 of EACEA</p> <p>Email: eacea-eplus-eve@ec.europa.eu</p>
5	Name and contact details of the Data Protection Officer (DPO)
	EACEA-data-protection@ec.europa.eu
6	Name and contact details of joint controller (where applicable)
	<p>The Education, Audiovisual and Culture Executive Agency is responsible for the management of Erasmus + Virtual exchange and joint controller together with the European Commission represented by the Directorate-General for Education, Youth, Sport and Culture. Contact details are those mentioned above.</p>
7	Name and contact details of processor (where applicable)
	<p>Consortium led by Search for Common Ground, rue Belliard 204, bte13, 1040 Brussels, tel. +32 2 736-7262 email: smelone@sfcg.org</p> <p>Other members of the contracted consortium are: The Anna Lindh Euro-Mediterranean Foundation for Dialogue and Culture, Unione della Università del Mediterraneo, Stichting Sharing Perspectives.</p> <p>In addition, a number of subcontractors also implement the project activities, including Soliya, UNICollaboration, Kiron open Higher Education, Zentrum für Angewandte Kulturwissenschaft und Studium Generale (ZAK), and Consult and Design.</p>
8	Purpose of the processing

	<p>Data processing is for the purpose of Erasmus+ Virtual Exchange project setup, registration for participation, implementation, quality control, monitoring and evaluation.</p> <p>Data is also processed for outreach and communication purposes within the framework of the Erasmus+ Virtual Exchange project, to disseminate information about the Erasmus+ Virtual Exchange project, solicit participation and establish partnerships with and among higher education institutions and youth organisations.</p> <p>In addition, personal data may be processed for the purpose of awarding an Erasmus+ Virtual Exchange badge to the participants, as recognition of the participation in the learning activity. Finally, for those participants who are enrolled in project activities through a partner institution, the data is used to provide feedback to partner institution on their students' or members' attendance and performance.</p>
9	<p>Description of the categories of data subjects</p> <p>Whose personal data are being processed? In case data categories differ between different categories of persons, please explain as well (e.g. suspects vs. witnesses in administrative inquiries)</p> <p><input type="checkbox"/> Agency staff (Contractual and temporary staff in active position)</p> <p><input type="checkbox"/> Visitors to the Agency</p> <p><input type="checkbox"/> Contractors providing goods or services</p> <p><input type="checkbox"/> Applicants</p> <p><input type="checkbox"/> Relatives of the data subject</p> <p><input type="checkbox"/> Complainants, correspondents and enquirers</p> <p><input type="checkbox"/> Witnesses</p> <p><input type="checkbox"/> Beneficiaries</p> <p><input type="checkbox"/> External experts</p> <p><input type="checkbox"/> Contractors</p> <p><input checked="" type="checkbox"/> Other, please specify:</p> <p>Participants who are interested in or register in Erasmus+ Virtual Exchange activities: student, youth worker, academic worker, young person not in higher education, facilitation trainee, facilitator, academic and higher education administration staff.</p>
10	<p>Description of personal data categories</p> <p>Indicate <u>all</u> the categories of personal data processed and specify which personal data are being processed for each category (between brackets under/next to each category):</p> <p>a) Categories of personal data:</p> <p><input type="checkbox"/> in the form of personal identification numbers</p> <p><input checked="" type="checkbox"/> concerning the physical characteristics of persons as well as the image, voice or fingerprints</p> <p>This refers to the photo that participants may choose to upload to their profile, and video assignments which are part of some activities.</p> <p><input checked="" type="checkbox"/> concerning the data subject's private sphere</p> <p>This refers to personal data that the participants may refer to themselves upon discussing (e.g. chats, fora) or carrying out their assignments (Videos/photos).</p>

	<div> <input type="checkbox"/> concerning pay, allowances and bank accounts <input type="checkbox"/> concerning recruitment and contracts <input type="checkbox"/> concerning the data subject's family <input type="checkbox"/> concerning the data subject's career <input type="checkbox"/> concerning leave and absences <input type="checkbox"/> concerning missions and journeys <input type="checkbox"/> concerning social security and pensions <input type="checkbox"/> concerning expenses and medical benefits <input type="checkbox"/> concerning telephone numbers and communications <input checked="" type="checkbox"/> concerning names and addresses (including email addresses) </div> <p>Personal data of those asking queries:</p> <p>Mandatory: name, email address, occupation (student, youth worker, academic worker, young person not in higher education, facilitation trainee, facilitator, contact point persons at partner institutions), city/country, interest/motivation in the activity.</p> <p>Optional: Telephone contact, name of organisation</p> <p>Registration data</p> <p>Mandatory: name, email address, telephone number, country of residence, nationality, gender, date of birth, occupation (student, youth worker, academic worker, young person not in higher education, facilitation trainee, facilitator, contact point persons at partner institutions), name of organisation/institution, region of origin (South Mediterranean or Europe), access to high speed internet, schedule availability for the duration of the programme, experience with or interest in virtual exchange or the proposed activity</p> <p>Optional: alternate e-mail address, skype ID, native language, additional languages spoken, if applicable graduation year and field of study, photo.</p> <p>Specifically the facilitators have to mandatorily provide current residence, language spoken, CV, cover letters and skype account.</p> <p><input checked="" type="checkbox"/> Other: please specify:</p> <p>Evaluation data on participants' attendance, participation and assignments in the activities.</p> <p>b) Categories of personal data processing likely to present <u>specific risks</u>:</p> <div> <input type="checkbox"/> data relating to suspected offences, offences, criminal convictions or security measures <input type="checkbox"/> data being used to evaluate personal aspects of the data subject (ability, efficiency, conduct) </div> <p>c) Categories of personal data whose processing is <u>prohibited</u>, with exceptions (art. 10):</p> <div> <input checked="" type="checkbox"/> revealing racial or ethnic origin <input checked="" type="checkbox"/> revealing political opinions <input checked="" type="checkbox"/> revealing religious or philosophical beliefs <input type="checkbox"/> revealing trade-union membership <input type="checkbox"/> concerning health <input type="checkbox"/> genetic data, biometric data for the purpose of uniquely identifying a natural person <input checked="" type="checkbox"/> concerning sex life or sexual orientation </div> <p>Registered users of the platform may reveal such personal data voluntarily while chatting</p>
--	---

	<p>or carrying out assignments (videos, photos).</p> <p>d) Specify any additional data or explanatory information on the data being processed, if any: If special categories of data are submitted by users on the platform (revealing racial or ethnic origin, political opinion, religious or philosophical beliefs) such data will be disregarded by the controller and its data processors.</p>
11	<p>Retention time (time limit for keeping the personal data)</p> <p>Indicate your <u>administrative retention period (CRL)</u> or – if not foreseen by it, a legal basis for it, or the agreed retention time, including its starting point; differentiate between categories of persons or data if needed (e.g. in selection procedures: candidates who made it into the reserve list vs. those who did not).</p> <p>Indicate the period of storage:....</p> <p>Personal data of those asking queries will be kept only as long as necessary and up to a maximum of 1 year, to respond to the query and/or expression of interest. They will be deleted after the processing, and, at the latest, 1 year after reception of the query/expression of interest. Where a mailing list has been signed up to, the user will be able to unsubscribe from that list at any time and the personal data will be kept until that time.</p> <p>Personal data contained within participants' and facilitators' user accounts on the virtual exchange platforms will become inactive 2 years after the user's last log-in and will immediately be anonymised.</p> <p>Chats that take place during the live sessions are deleted at the end of each session. Posts and contributions on forums, as well as videos exchanged on the platforms during the project will be deleted 1 year after the end of each project activity. All data collected regarding the participants' attendance and completion of assignments will be anonymized 1 year after the end of each project activity, after the Erasmus+ Virtual Exchange recognition badges have been awarded.</p> <p>Minimised data about youth participants (name, e-mail) will be kept based on consent (opt-in), to ensure the continued engagement with alumni, propose participation in future programmes and trainings, and keep alumni informed about the project.</p> <p>All data collected for the monitoring and evaluation of the activities, including the surveys, questionnaires and interviews, are anonymised prior to any processing for analysis.</p> <p>Personal data of facilitators and trainers will be deleted 2 years after they cease being active in the Erasmus+ Virtual Exchange project. Their photo and short biography will cease being public/visible on the Hub.</p> <p>Minimised data about facilitators and trainers (name, email, gender, nationality, country of residence, languages spoken, as well as past performance data) will be retained, on the basis of consent (opt-in), for the continuity of the project and in order to solicit participation in future programmes.</p> <p>Participants and facilitators can delete their profiles themselves at any moment. Users deleting their own profile will result in immediate and unrecoverable anonymization of their profiles and all LMS (Learning Management System) data, as well as manual anonymization of their records held in storage.</p> <p>Is any further processing for historical, statistical or scientific purposes envisaged? <input checked="" type="checkbox"/> yes <input type="checkbox"/> no</p> <p>If yes, indicate the further retention time:</p>

	<p>Data is immediately anonymised prior to processing for analysis.</p> <p>If the answer is yes, please go to Part 2, Storage and Security for technical safeguards.</p>
12	<p>Recipients of the data</p> <p>As a participant or a facilitator, basic data, user-generated content, contributions and comments posted onto the platforms will be visible to the other users of the exchange platforms.</p> <p>The photos and biographies of Erasmus+ Virtual Exchange Facilitators, who have provided their consent to post this information on the Erasmus+ Virtual Exchange Hub, will be visible for the general public.</p> <p>Access to personal data may be given on a need-to know basis to the following recipients:</p> <ul style="list-style-type: none"> • EACEA and DG EAC designated staff; • Authorised staff of the consortium of organisations contracted by the EACEA to implement the project activities (see point 7 above), i.e. Search for Common Ground, Anna Lindh Euro-Mediterranean Foundation for Dialogue between Cultures, Unione delle Università del Mediterraneo (UNIMED) and Stichting Sharing Perspectives (SPF), and their subcontractors, including Soliya, UNICollaboration, Zentrum für Angewandte Kulturwissenschaft und Studium Generale (ZAK), and Consult and Design. <p>In addition, transfers of personal data to the following third parties and countries can take place in the context of the Erasmus+ Virtual Exchange project, on a need-to-know basis. Such transfers are done with appropriate safeguards, referenced below. You may request to obtain a copy of them by contacting the controllers as indicated under point 1 above.</p> <ul style="list-style-type: none"> • Authorised Soliya staff, based in the US. Soliya is certified under the EU-US Privacy Shield. Confidentiality is further ensured through a non-disclosure agreement; • Authorised Soliya staff of the Tunisia branch. Confidentiality is ensured through a Commitment on the Processing of Personal Data for the Project Erasmus+ Virtual Exchange. Confidentiality is further ensured through a non-disclosure agreement. • Facilitators/trainers, located anywhere in the world. Confidentiality is ensured through a non-disclosure agreement; • Partner institutions, located in any eligible country, who only receive data in relation to the students/members coming from their own institutions. Confidentiality is ensured through a data protection clause in the Memorandum of Understanding signed between the consortium and these institutions; • Processors engaged by the consortium, including the following cloud storage providers: GSuite, SurveyMonkey, Nomadesk, Mailchimp, Live Agent, Drupal, Amazon. For those based in the US (such as GSuite, Mailchimp and Amazon), they are all certified under the EU-US Privacy Shield. <p>The transfer of data to other third parties is prohibited. Personal data collected will never be used for marketing purposes.</p>
13	<p>Are there any transfers of personal data to third countries or international organisations? If so, to which ones and with which safeguards?</p> <p><i>Example: processor in a third country using an adequacy decision, standard contractual clauses, binding corporate rules, a third country public authority you cooperate with based on existing legislation/agreement. If needed, consult your DPO for verifying the legal basis and for more information on how to ensure safeguards.</i></p>

	<p>As mentioned under point 12 above, transfers of personal data to subcontractors can take place in the context of the Erasmus+ Virtual Exchange project, on a need-to-know basis:</p> <ul style="list-style-type: none"> - Soliya, US entity: EU-US Privacy Shield. In addition, all staff members handling/processing personal data sign non-disclosure agreements. - Soliya branch in Tunisia: Staff members handling/processing personal data sign non-disclosure agreements. Commitment on the Processing of Personal Data for the Erasmus+ Virtual Exchange Project signed between Soliya HQ and its Tunisia branch. <p>Moreover, transfers of personal data can be made to:</p> <ul style="list-style-type: none"> • Facilitators/trainers/debate team leaders may be anywhere in the world: Facilitators/trainers/debate team leaders have access to limited participant/trainee data (name, email, telephone number, gender, nationality, data on attendance/performance). Non-disclosure agreement is signed by facilitators, trainers and debate team leaders. • Partner institutions, which may be in any eligible country: Evaluation data on participants' attendance, participation and assignments in the activity is transferred to partner institution from which the participants belong. They receive such data only in relation to the students/members coming from their institution. Data protection clauses in the Memorandum of Understanding have been signed between the consortium and partner institutions.
14	<p>General description of the technical and organisational security measures</p> <p>Include a general description of your technical and organisational security measures that you could also provide to the data subjects and general public.</p> <p>Organisational Measures</p> <p>Organisational measures include appropriate access rights and access control.</p> <p>The data is physically stored in the Commission (Youth Portal) secure web-based servers and servers of the project promoters (consortium partners).</p> <p>Participant data may be transferred securely to software such as:</p> <ul style="list-style-type: none"> - EVE Hub, hosted on the EACEA Youth Portal - Live Agent – server located in the United Kingdom. - MailChimp – server located in the United States. (privacy shield: https://www.privacyshield.gov/participant?id=a2zt00000000TO6hAAG) - Soliya Exchange Portal and LMS (Learning Management System), hosted on Amazon – server located in Frankfurt. - Nomadesk - servers located in Amsterdam and Frankfurt. - UNICollaboration Moodle platform, hosted on Aruba – server located in Italy. - Sharing Perspective Foundation Videologue platform, Drupal web application – server located in Amsterdam. - G-Suite – servers in multiple locations, data stored in the EU if the account holder is EU-based, and in the US if the account holder is US-based. (privacy shield: https://www.privacyshield.gov/participant?id=a2zt000000001L5AAI) - Learning Management System by provider Instructure, Inc. (Canvas) – server located in the United States. (privacy shield: https://www.privacyshield.gov/participant?id=a2zt00000000TREVAAO&status=Active) - SurveyMonkey – server located in the United States. (privacy shield: https://www.privacyshield.gov/participant?id=a2zt00000000Gn7zAAC) <p>All software used would be hosted either in the EU or in the US (with Privacy Shield Authorisation) and would be behind secure password-protected environments in line with the General Data Protection Regulation.</p> <p>At the Agency level, access to personal data is restricted to staff members on a need to know basis.</p>

	<p>The service contract with Search for Common Ground and its partners includes a data protection clause.</p> <p>The service provider demonstrated to the Agency that he takes Data Protection issues seriously and has instituted some specific measures to review how personal data is collected and managed in the consortium and also to raise awareness of the staff with respect to privacy issues.</p> <p>In particular</p> <ul style="list-style-type: none"> • Data mapping and Erasmus+ Virtual Exchange protection and security guidelines for the Erasmus+ Virtual Exchange project have been developed (see supporting documents), with the support of a subcontracted consultant in data protection and privacy, CRANIUM Belgium NV, to ensure compliance of all consortium members with the applicable legislation. These include a number of organisational measures to be applied by consortium members processing data in the context of the project, including on data access management. Further measures will be developed over the course of 2019, with the support of CRANIUM (a consultancy firm specialised in data protection and cybersecurity), to continue supporting consortium members in enhancing data management and security. • Two dedicated data protection training sessions were conducted on 27 June 2018 and 5 October 2018 with all staff involved in the implementation of Erasmus+ Virtual Exchange activities. • Agreements with subcontractors include a data protection clause. Transfers to third countries are bound by adequate legal arrangements to ensure safeguards (see point 13). • Staff members who conduct data collection and processing activities are subject to a Non-Disclosure Agreement with regard to the processing of personal data. <p>Technical Measures</p> <p>Technical measures include the use of secure equipment (e.g. locked cupboards) and IT-tools (including secure connections, firewalls, etc.).</p> <p>The following measures have been taken, with the aim of:</p> <p>(a) preventing any unauthorised person from gaining access to computer systems processing personal data;</p> <p>All computer systems including phones, tablets and computers accessing personal data are utilising strong password access and in many cases biometric access. Online platforms used as part of the project use password protected access, where possible two-factor authentication access, and permission systems to prevent anyone but those authorised any access to personal data.</p> <p>(b) preventing any unauthorised reading, copying, alteration or removal of storage media;</p> <p>We have prioritised all personal data to be hosted in Software as a Service solutions to decrease the risk levels of having files in different locations. Where files are created using personal data these are strongly password protected and require digital shredding when no longer required. Where personal data is held in databases relevant firewalls have been implemented.</p> <p>(c) preventing any unauthorised memory inputs as well as any unauthorised disclosure, alteration or erasure of stored personal data;</p> <p>Software used has lifetime change management tools that detail every change made to the data and by which data processor. Permission management means that deletion can only take place at the highest level or by users themselves.</p> <p>(d) preventing unauthorised persons from using data-processing systems by means of data</p>
--	--

	<p>transmission facilities;</p> <p>Only a limited number of named individuals (maximum 3) within each of the consortium partners have access to the highest level of permission in information systems, and where personal data is stored in a document or database it is only on a needs-access basis. By ensuring that the lowest number of users have access to the information systems we ensure the lowest level of risk.</p> <p>The Erasmus+ Virtual Exchange consortium members take steps to prevent any unauthorised person from gaining access to computer systems processing personal data:</p> <ul style="list-style-type: none"> • The granting and modification of access rights must be based on: the authorized personnel's responsibilities, job duty requirements necessary to perform authorized tasks; and a need-to-know basis; • All computer systems including phones, tablets and computers accessing personal data must use strong password access. Password policies that follow at least industry standard practices must be implemented, including password expiry, restrictions on password reuse and sufficient password strength; • Online platforms used as part of the project use password protected access and permission systems to prevent anyone but those authorised any access to personal data; • Any root and administrator passwords should only be held by individuals who absolutely require them in order to successfully carry out server administration requirements. Any passwords at the server level should be held in password protected environments and should never be written down or shared; • To create an audit trail for accountability, server and/or software technical logs should be implemented that allow changes in data to be logged to a specific user, and should be made available for a minimum of 3 months and ideally up to 12 months. Logs must not contain any personal data but should identify the data that has been updated; • Regular reviews of access permissions should be carried out to assess and update staff and subcontractor access on a need-to-know basis; <p>(e) ensuring that authorised users of a data-processing system can access no personal data other than those to which their access right refers;</p> <p>The personal information we request is of the nature that if you have personal data access to the systems, you have access to all the data. This ensures there is no confusion around levels of access. Only a small number of users for each system have access to the highest level of data processing and permission granting options.</p> <p>(f) recording which personal data have been communicated, at what times and to whom;</p> <p>All actions taken on all data systems (Live Agent, GSuite, Live Agent, Platforms) are done so with user-linked tracking that provides a record of all changes made, when and by whom.</p> <p>(g) ensuring that it will subsequently be possible to check which personal data have been processed, at what times and by whom;</p> <p>See answer to f).</p> <p>(h) ensuring that personal data being processed on behalf of third parties can be processed only in the manner prescribed by the contracting institution or body;</p> <p>The Erasmus+ Virtual Exchange data protection guidelines have been put in place to ensure compliance with the Regulation (EU) 2018/1725, as well as the data protection clause in the service contract 2017-3620/001-001. Contractual arrangements between Erasmus+ Virtual Exchange (EVE) contractors and their subcontractors are in place, including a data protection clause. EVE consortium members ensure that all trainers and facilitators working in the context of the EVE project sign the EVE Non-Disclosure Agreement prior to handling any personal data.</p>
--	--

	<p>(i) ensuring that, during communication of personal data and during transport of storage media, the data cannot be read, copied or erased without authorisation.</p> <p>Data in transit is encrypted via SSL/TLS, management access and data transfers on platforms are done securely via SSH and SFTP only.</p>
15	<p>Information to data subjects / Privacy Statement</p> <p>A privacy statement including specific mention to the EU regulation on this subject is available on the Hub for Erasmus+ Virtual Exchange, as well as on external websites where participants can register.</p> <p>The web forms on the Hub and online registration on the activity platforms cannot be completed without ticking the box asking for agreement to the privacy statement.</p> <p>The privacy statement is permanently available on the Hub and on all activity platforms.</p>