EUROPEAN EDUCATION AND CULTURE
EXECUTIVE AGENCY (EACEA)

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 nº 09-2020

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

This record covers two aspects:

1. Mandatory records under Art 31 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*
☐ *Migration from notification to record.*

General online training operation	
1	**Last update of this record (where applicable)**
	First version : 27/08/2020
2	**Short description of the processing**
	The processing of personal data in the frame of the General Online Training (GOT) is required to allow the European Solidarity Corps (ESC) registered users in the European Youth Portal to gain access to and participate in the General Online Training (GOT) courses available on EU Academy platform. Moreover the processing has the purposes of undertaking an aggregated analysis of responses to the satisfaction surveys collected via the EU Academy platform and of collecting statistics and reports in anonymised format on the use of the GOT courses.
Part 1 - Article 31 Record	
3	**Name of the Controller** **Unit(s) and/or function of person acting on behalf of the Controller**
	Controller: European Education and Culture Executive Agency

	Unit A5: Youth, EU Solidarity Corps and Aid Volunteers Head of Unit, EACEA-SOLIDARITY-CORPS@ec.europa.eu
4	**Contact details of the Data Protection Officer (DPO)** EACEA-data-protection@ec.europa.eu
5	**Name and contact details of joint controller (where applicable)** The European Commission represented by the Directorate-General for Education, Youth, Sport and Culture (DG EAC.B3 Youth, Volunteer Solidarity and Traineeships Office) Email address: EAC-DATA-PROTECTION-COORDINATOR@ec.europa.eu .
6	**Name and contact details of processor (where applicable)** ICF SA Email: esc.got@icf.com UP learning, partner in the ICF consortium Email: security@uplearning.nl
7	**Purpose of the processing** Date processing is necessary for the following purposes: All personal data processing via EU Academy is made in accordance with the EU Academy Privacy Statement. A. To ensure access for European Solidarity Corps registered users to the set of courses of the European Solidarity Corps General Online Training hosted on EU Academy and to enable reporting for the European Solidarity Corps services of DG EAC and EACEA, as well as to be able to present an aggregated analysis of course usage, by key characteristics of users, in a monthly statistical report. B. To be able to present an aggregate analysis of the survey responses, including by key characteristics of respondents, in a monthly statistical report. The data is anonymised for this purpose. C. To monitor users' progresses and for statistical purposes in dedicated reports. The data is anonymised for this purpose. D. To realise video streaming, video recording, photo shooting, creation in post-production of the Youth talks videos. Processing of personal data via the European Commission's YouTube channel, where the Youth talks are available will be made in accordance with the data protection record: DPO Public register (europa.eu) . E. To collect interest, evaluate and select speakers for the Youth talks series, including communication purposes, such as invitation letters and direct communication related to the event at which you have been selected to speak at, registration purposes to the event at which you have been selected to speak at, for the production of live-streaming and post-event video production and publication of those videos on the European Commission's YouTube channel, the General Online Training platform, the EU Academy and the European Youth Portal.
8	**Description of the categories of data subjects** 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) ☐ Agency staff (Contractual and temporary staff in active position)

	☐ Visitors to the Agency ☐ Contractors providing goods or services ☐ Applicants ☐ Relatives of the data subject ☐ Complainants, correspondents and enquirers ☐ Witnesses ☐ Beneficiaries ☐ External experts ☐ Contractors ☒ Other, please specify: All registered users on the European Solidarity Corps Youth Portal, speakers in the Youth talks series, the audience of the Youth talks events who accepted to be filmed.
9	**Description of personal data categories**
	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): ***a) Categories of personal data:*** ☐ in the form of personal identification numbers ☐ concerning the physical characteristics of persons as well as the image, voice or fingerprints ☒ concerning the data subject's private sphere ☐ concerning pay, allowances and bank accounts ☐ concerning recruitment and contracts ☐ concerning the data subject's family ☐ concerning the data subject's career ☐ concerning leave and absences ☐ concerning missions and journeys ☐ concerning social security and pensions ☐ concerning expenses and medical benefits ☒ concerning telephone numbers and communications ☐ concerning names and addresses (including email addresses) ☒ Other: please specify: 1. European Solidarity Corps registered users' data indicated below are transferred from the European Youth Portal to EU Academy: □ Email (mandatory) □ EU Login username (mandatory) □ First name (mandatory) □ Last name (mandatory) □ Contact language (mandatory) □ Country of residence (mandatory)

	City (optional) 2. If the user agrees to respond to the online feedback survey on EU Academy after the course completion, the GOT data controller and data processor (external service provider contracted by EACEA) may have access to these data to realise anonymised customised reports. 3. The following data available on EU Academy may be processed by the GOT data controller and data processor (external service provider contracted by EACEA): courses access and course completion data, course enrolment, course progress data. These data will be used in an aggregated and anonymised manner, for monitoring progresses and statistical purposes 4. The following personal data are processed in the context of the General Online training services for European Solidarity Corps Participants Call for Expression of interest for the Youth Talks through the application form Qualtrics. • Mandatory data: • First name • Last name • Age • Email Address • Nationality • Country of residence • Experience in public speaking • Details of your story to be conveyed in a Youth Talk speech • A video of you pitching the speakers and their idea to become a Youth Talk speaker In addition, for the speakers who are selected: • Speaker's images from the Youth event for the live-streaming, the production of post-event video and for sharing it on European Commission's YouTube channel, the General Online Training platform, the EU Academy and the European Youth Portal. Optional data: • The opinions shared by speakers might reveal their own political opinions. However, this is not the purpose of the Youth talks event, and these data are not required by the organiser. Therefore such opinions/data are shared by the speakers on their own decision/on a voluntary basis. ***b) Categories of personal data processing likely to present <u>specific risks:</u>*** ☐ data relating to suspected offences, offences, criminal convictions or security measures ☐ data being used to evaluate personal aspects of the data subject (ability, efficiency, conduct) ***c) Categories of personal data whose processing is <u>prohibited</u>, with exceptions (art. 10):*** ☐ revealing racial or ethnic origin ☐ revealing political opinions ☐ revealing religious or philosophical beliefs ☐ revealing trade-union membership ☐ concerning health ☐ genetic data, biometric data for the purpose of uniquely identifying a natural person ☐ concerning sex life or sexual orientation

	d) Specify any additional data or explanatory information on the data being processed, if any: N/A
10	**Retention time (time limit for keeping the personal data)**
	For the purposes set out in A, B, and C, the period of storage, including access logs, is in line with the retention period of the European Youth Portal: personal data contained within user accounts of the European Solidarity Corps will be deleted three years after they reach the upper age limit of eligibility for participation in the Corps, unless the user has agreed to join any alumni scheme that may be in place at that time, has expressed via email an interest in keeping the user account or has benefited from EU funding through participating in the programme in which case the data is kept for 5 years from the last financial transaction according to the common retention list. Online consultation processes contributions will be anonymised (i.e. the link between the user and the contributions / votes they made will be removed) within two years after the end of each complete consultation and reporting / feedback process. The retention policy of EU Academy may also have an impact on the GOT retention policy. For the purpose set out in D, the EC YouTube channel retention policy is applicable. For the purposes set out in E, data relating to registrants who are not selected will be deleted right after the selection deadline by the contractor for the provision of the European Solidarity Corps General Online Training. For the selected participants, personal information (Cvs, motivation letters, personal contact details, etc.) will be kept until the publication of the post-event video to the European Commission's YouTube channel. The Youth talk videos as post-produced after the event will be inserted on the General Online Platform and they will be subject to the General Online training retention period policy. The consent of the data subject is required as indicated in the Statement of consent for processing of personal data, included in the registration form. **Is any further processing for historical, statistical or scientific purposes envisaged?** ☐ yes ☒ no **If yes, indicate the further retention time:** N/A
11	**Recipients of the data**
	Access to personal data may be given on a need-to know basis to the following recipients: – Designated staff of the European Commission, Directorate General Education and Culture (DG EAC) – Designated staff of the European Commission, JRC, EU Academy team – Designated staff of EACEA – Authorised staff of the contractor of the Framework services contract n° SI2.1334: consortium between ICF S.A., ICF Next S.A. UP learning B. V., MDF Training & Consultancy B.V, in particular System Administrators and technical engineers of UP learning, ICF project staff, MDF project staff, and the contractors who will replace them at the end of the contract. The transfer of data to other third parties is prohibited. Personal data collected will never be used for marketing purposes

	In addition, in case of control or dispute, personal data can be shared with and processed by the bodies charged with a monitoring or inspection task in application of Union law in compliance with the applicable data protection rules and within the scope of their tasks entrusted by the relevant legislation. This includes, in particular, the following recipients: - The European Court of Justice or a national judge as well as the lawyers and the agents of the parties in case of a legal procedure; - The European Anti-Fraud Office (OLAF); - The Internal Audit Service of the Commission - The Investigation and Disciplinary Office of the Commission (IDOC) - The European Court of Auditors - The European Ombudsman - The European Public Prosecutor's Office - EU courts and national authorities
12	**Are there any transfers of personal data to third countries or international organisations? If so, to which ones and with which safeguards?** Personal data processed by the contractor ICF S.A. will be processed in the European Economic Area (EEA) and in the United Kingdom. Based on the decision on the adequate protection of personal data by the United Kingdom, adopted on 28 June 2021, personal data can flow from the EU to the UK without any further safeguard being necessary.
13	**General description of the technical and organisational security measures** European Youth Portal is under the responsibility of DG EAC (for purpose A), and the applicable measures are described in the dedicated data protection record. EU Academy is under the responsibility of JRC (for purposes B and C) and the applicable measures are described in the dedicated data protection record (DPR-EC-05546). UP learning (for purpose B, C and D) The data centre in the Netherlands and is not cloud based. The datacentre is Tier3 equivalent certified and ISO/IEC 27001 and NEN 7510 certified. Physical and network access to the backend is only allowed for designated technical engineers of UP learning. UP is an ISO 27001 certified company and has implemented an Information Security Management Systems (ISMS). The scope of the ISMS focusses on develop, deliver and manage online learning solutions as adopted by the management of UP and in accordance with the Statement of Applicability version 2.0 (available at UP on request). Reporting obligation data leaks and security breaches In case of a suspected or actual (i) data leak; (ii) breach of security; (iii) breach of confidentiality or (iv) loss of confidential data UP Learning will immediately, or within 48 hours, inform EACEA after the initial discovery of the incident. UP will take all reasonable measures as per IT security plan at Part 6, point 2 of this data protection record, necessary to prevent (further) unauthorized inspection, modification and distribution or to prevent otherwise unlawful processing or reduce and terminate a breach of security, breach of confidentiality or further loss of confidential data and in the future, without prejudice to any right of the customer to compensation or other measures. ICF (for purpose B, C and D): ICF is an ISO27001 accredited organisation. Data security is managed in accordance with ICF's Information Security policy which details comprehensive measures relating to: physical security, communications and operations management including network security management; access control including review of access rights, user authentication of external connections, equipment identification in networks, remote diagnostic and confirmation port protection and segregation in networks, incident management and business continuity management. ICF currently use Symantec Net Share for the secure storage and transfer of relevant sensitive data. On receipt, such sensitive electronic data is encrypted and held on a secure server, with access to it being restricted to members of specific project teams (using access control lists). No sensitive information is stored on the researcher's hard drives or other portable media - although all corporate endpoints are deployed with full disk encryption to

	mitigate the potential for data loss. All ICF's premises sit behind enterprise firewalls that restrict inbound and outbound traffic to authorised traffic and apply intrusion detection. In circumstances where full isolation is required, data is securely stored on a separate device that is removed from all network access (both internal and external [internet]). All systems require password authentication to access. Company policy dictates use of a 9-character minimum length, a mix of character types and this must be changed every 30 days. ICF has well developed procedures in place to ensure the secure transfer of sensitive electronic data between itself, clients and subcontractors where appropriate. Where sensitive data is transferred, we use secure email, which allows encrypted data files to be emailed using public key cryptography. Where this is not possible, we have several alternatives including authenticated transfer via TLS from corporate file share servers. The European Commission's IT systems used by the Agency abide by the Commission's security guidelines. The Agency must comply with Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission. 1. Organisational measures: A Corporate Local Informatics Security Officer (C-LISO) is in place. Its role includes supervising the Agency compliance with the relevant regulations, and the application of security measures recommend by DIGIT. Organisational measures include appropriate access rights and access control. As a rule within the Agency, access to information systems, the file system or offices are subject to a series of authorisations where the person granting the access is different from the person requesting or authorising the access - except in limited cases of delegation. The responsible person in the unit in charge of this action (processing operation of the current record) collects and places the documents on the secured drives of the Commission and all Agency staff are bound by a confidentiality obligation. The need to know principle applies in all cases. 2. Technical measures: State of the art technical cybersecurity measures are implemented in the corporate systems, according to the security needs. Those measures are in constant evolution.
14	**Information to data subjects / Data Protection Notice (DPN)**
	European Solidarity Corps Portal : **GOT DPN on EYP DPN** GOT data protection notice: **GOT-DPN** For the Youth talks, a dedicated DPN is made available to the data subjects (applicants to the call for expression of interest to become Youth talks speakers and to the audience of the events where the Youth talks are registred).

ANNEX

When to perform a Data Protection Impact Assessment (DPIA)

- **Data Protection Impact Assessment (DPIA)**

  You will not have to do DPIAs for all processing operations. Only those that are likely to pose a 'high risk to the rights and freedom of data subjects' require a DPIA. As the person responsible on behalf of the controller, preparing the DPIA is your task, assisted and guided by the DPO.

  The EDPS shall establish and make public a list of "kinds of processing operations" subject to a DPIA. The EDPS may also establish a negative list of kinds of processing operations not subject to DPIAs.

  You have to carry out a DPIA when your process meets at least one of the criteria below:

  (1) it is on the list of kinds of risky processing operations to be issued by the EDPS;
  (2) it is likely to result in high risks according to your threshold assessment

- **Threshold assessment**

  For processing operations that do not figure on the list for mandatory DPIAs, but which you and/or DPO still suspect may be high risk, conduct a threshold assessment using the template included in this document. In general, if you tick two or more of the criteria, you should do a DPIA. However, the assessment cannot be reduced to a simple calculation of the number of criteria met. This is not an automated decision. Indeed, in some cases, a processing meeting only one of these criteria may require a DPIA. In other cases, a DPIA may not be necessary despite meeting two or more criteria. If you tick two or more criteria and do not consider that the processing would in fact cause high risks for the persons affected, explain why after consulting the DPO.

- **EDPS Positive/negative lists**

  Below you may find the positive and negative lists (indicative) issued by EDPS. These lists are non-exhaustive (and not yet official) and aim at providing some guidance in the interim period.

  A) Positive list of processing operations prima facie requiring a DPIA (the numbers in brackets refer to the criteria in the threshold assessment such processing operations will likely trigger):

- Exclusion databases (2, 4, 9);
- large-scale processing of special categories of personal data (such as disease surveillance, pharmacovigilance, central databases for law-enforcement cooperation) (1, 4, 5, 8);
- internet traffic analysis breaking encryption (1, 3, 8).

B) Indicative list of processing operations prima facie *not* requiring a DPIA:

- Management of personal files as such[1];
- Standard staff evaluation procedures (annual appraisal);
- 360° evaluations for helping staff members develop training plans;
- Standard staff selection procedures;
- Establishment of rights upon entry into service;
- Management of leave, flexitime and teleworking;

[1] Some procedures resulting in adding information to the personal file may require DPIAs, but not the repository of personal files as such.

- Standard access control systems (non-biometric);
- Standard CCTV on a limited scale (no facial recognition, coverage limited to entry/exit points, only on-premises, not in publicly accessible space).