Ref. Ares(2023)7506932 - 06/11/2023

EUROPEAN COMMISSION
European Education, 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 nº *2023-08*

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.*

Erasmus+ National Erasmus Offices (NEOs)	
1	**Last update of this record (where applicable)** N/A
2	**Short description of the processing** We will process personal data in order to establish a network of National Erasmus Offices (NEOs) covered by the European Enlargement and Neighbourhood Policy (Albania, Armenia, Azerbaijan, Bosnia and Herzegovina, Georgia, Kosovo*, Moldova, Montenegro, Ukraine, Israel, Jordan, Lebanon, Palestine**, Kazakhstan, Kyrgyzstan, Tajikistan, Turkmenistan, Uzbekistan, Algeria, Egypt, Libya, Morocco, Tunisia). * All references to Kosovo should be understood in the context of UNSCR-1244(1999) **This designation shall not be construed as recognition of a State of Palestine and is without prejudice to the individual positions of Member States on this issue The purpose of the network is to create a support structure that will be an essential component in the implementation of the Erasmus+ programme (2021-2027). The

	individual representing the NEOs will provide information and on-the-ground advice to potential applicants and beneficiaries. They will have a key role in supporting the Erasmus+ programme's objectives and impact by ensuring that it becomes known and readily accessible to all potential applicants, irrespective of the sector. The contact information of individuals representing the NEOs will not be made public by EACEA but used only for networking within that group, for exchanging relevant information, and documents and for meetings with the EACEA, other Commission services (e.g. EU Delegations). It is foreseen that the NEOs and the above-mentioned institutions and individuals will meet at networking events online and in person. A specific TEAMs channel will be also put in place for the NEO. The individual NEOs can be reached via the Erasmus+ webpage managed exclusively by DG EAC (National Erasmus+ Offices | Erasmus+ (europa.eu)).
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(s): A4 EACEA-EPLUS-NEO-HERES@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)** N/A
6	**Name and contact details of processor** **(where applicable)** NETCOMPANY - INTRASOFT S.A. 2B Rue Nicolas Bové 1253 Luxembourg, Luxembourg Contact | Netcompany-Intrasoft
7	**Purpose of the processing** The information is collected in order to be able to contact the NEOs and to establish a network so the NEOs can communicate with each other. Moreover, the NEOs can be contacted by EACEA, other EU institutions for networking and communication purposes, programme implementation and monitoring purposes. The NEOs will be nominated by the competent authorities in each country, often the national Ministry of Education. This information is communicated to the EU Delegation in the country. The latter informs the EACEA about the nomination. EACEA is responsible for storing the contact information and updating the information when necessary. It is EACEA's purpose to keep the contact details of the individuals representing the NEOs in order to be able to contact the network and to be able to establish and animate a network within the NEOs. The contact information of individuals representing the NEOs will not be made public by EACEA but used only for networking within that group, for exchanging relevant information and documents and for meetings with the EACEA, other Commission services (e.g. EU Delegations). It is foreseen that the NEOs and the above-mentioned institutions and individuals will meet at networking events online and in person. A specific TEAMs channel will be also put in place for the NEO. The individual NEOs

	can be reached via the Erasmus+ webpage managed exclusively by DG EAC (National Erasmus+ Offices | Erasmus+ (europa.eu)). The framework of the MS Teams collaborations is defined in the data protection record for the European Commission's Microsoft 365 environment (reference No. DPR-EC-04966.4). The personal data of registered members will not be used for any automated decision-making including profiling.
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), Commission and EU Delegation Staff joining the TEAMS group ☐ 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: individuals nominated by competent national authorities (often Ministries of Education) from non-EU countries (namely, the NEO staff), Higher Education Reform Experts (HERE), Erasmus National Focal Points (ENFPs), Staff Members of National Agencies and other participants).
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 and voice ☐ 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 (position and name of employer) ☐ concerning leave and absences ☐ concerning missions and journeys ☐ concerning social security and pensions ☐ concerning expenses and medical benefits ☒ concerning telephone numbers and communications (telephone numbers and email addresses)

	☒ concerning names and addresses (including email addresses) (names and email addresses) ☒ Other: please specify: title, academic title, gender, institution type, institution name, institution location, present position. Furthermore, whilst using the discussion forum function of the platform/MS Teams, data subjects can also submit any other personal data voluntarily. _________ ***b) Categories of personal data processing likely to present specific risks:*** ☐ 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 prohibited, 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: _________***
10	**Retention time (time limit for keeping the personal data)**
	Indicate the period of storage: EACEA will keep the data in the restricted U-Drive and in Microsoft TEAMS until either the individuals representing NEOs wants to delete the information, until the national authority will change especially the legal representative, or until the NEO network ceases to exist (at least, until the end of the current MFF 2021-2027). The data needs to be stored for this duration because the EACEA needs to have means to be able to reach out to the NEOs and to ensure that they can network with each other. For health data (allergies, accessibility), EACEA will delete them as soon as they are not needed after the concerned event. **Is any further processing for historical, statistical or scientific purposes envisaged?** ☐ yes ☒ no **If yes, indicate the further retention time:** If the answer is yes, please go to Part 2, Storage and Security for technical safeguards.
11	**Recipients of the data**
	Personal data will be made accessible on need to know basis to the authorised staff within the following recipients: - EACEA, - European Commission services, in particular DG EAC, INTPA, NEAR, - EU Delegations in third countries, - European External Action Service,

Some personal data of the users of MS Teams (HEREs, Staff of Erasmus+ National Agencies and Erasmus+ National Offices (NEOs), EACEA and DG EAC staff) is visible by other users of the MS TEAMs.
These recipients include all the above and the:
- Erasmus+ National Agencies,
- Erasmus+ National Offices (NEOs)

Furthermore, by joining MS Teams email address and name will be accessible to the entire network through MS Teams.

Third party tools potentially used:

- Beyond (BeyondLive | Virtual Events Platform | Beyond Live | BeyondLiveX.com) will process your data as separate controller for streaming online live events and show recordings, in accordance with its privacy policy which can be found here: Privacy Policy | BeyondLive (beyondlivex.com). We draw your attention to international transfers which might be carried out.
- B2match will process your data as separate controller for the purpose of carried out the web streaming online live events and show recordings on the following website Event Platform Built for Networking (b2match.com). For this purpose, you personal data will be processed in accordance with its privacy policy: Privacy Policy (b2match.com)
- Aventri (https://www.aventri.com) as registration tool provide will process your data as separate controller for the purpose of organising and managing the event, in accordance with its privacy policy which can be found here: https://www.aventri.com/privacy-policy. We draw your attention to international transfers which might be carried out.
- Microsoft Teams: images and video recordings of the event may be published on the specific Microsoft TEAMS channel and processedin accordance with the following privacy policy (https://ec.europa.eu/dpo-register/detail/DPR-EC-04966).
- Slido: to allow participants to interact and ask questions. Your personal data used for your participation to the event will also be processed by this tool, in accordance with its privacy policy which can be found here: https://ec.europa.eu/dpo-register/detail/DPR-EC-06687. Participants not willing to share their personal data with Slido can simply use it by using their organisation's name or other anonymous data to submit questions via the tool.
- EU Survey (EUSurvey - Welcome (europa.eu)) as registration tool will provide will process your data for the purpose of organising and managing the event, in accordance with its privacy policy which can be found here: https://ec.europa.eu/eusurvey/home/privacystatement

In addition, data may be disclosed to public authorities, and processed by these authorities in compliance with the applicable data protection rules according to the purpose of the processing, including inter alia:

- 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 competent Appointing Authority in case of a request or a complaint lodged under Articles 90 of the Staff Regulations;
- OLAF in case of an investigation conducted in application of Regulation (EC) No 1073/1999;
- The Internal Audit Service of the Commission within the scope of the tasks entrusted by article 118 of the Financial Regulation and by article 49 of the Regulation (EC) No 1653/2004;
- IDOC in line with Commission Decision of 12 June 2019 laying down general implementing provisions on the conduct of administrative inquiries and disciplinary proceedings - C(2019)4231 and Commission Decision (EU) 2019/165 of 1 February 2019 Internal rules concerning the provision of information to data subjects and the restriction of certain of their data protections rights in the context of administrative inquiries, pre-disciplinary, disciplinary and suspension proceedings;

	- The Court of Auditors within the tasks entrusted to it by Article 287 of the Treaty on the Functioning of the European Union of the EC Treaty and Article 20, paragraph 5 of Regulation (EC) No 58/2003; - The European Ombudsman within the scope of the tasks entrusted to it by Article 228 of the Treaty on the Functioning of the European Union; · The European Public Prosecutor's Office within the scope of Article 4 of Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office.
12	**Are there any transfers of personal data to third countries or international organisations? If so, to which ones and with which safeguards?**
	Please note that in order to deliver the service, Microsoft Teams might transfer your personal data outside the EU as indicated in the data protection record of the Commission (https://ec.europa.eu/dpo-register/detail/DPR-EC-04966). Such transfer will be made based on standard contractual clauses as part of a contract between the service provider and the European Commission. You can obtain more information on it by contacting the data controller at the above-mentioned email address.
13	**General description of the technical and organisational security measures**
	1. Organisational measures: 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. For confidential files, access to documents is also limited based on a need to know rule. The access to the EACEA building is protected and only persons with the right to enter are allowed. All computers are password-secured. Access to the functional mailbox used for this purpose is given to a restricted number of staff on a need-to-know basis and all staff are bound by confidentiality obligations and other related legal obligations. 2. Technical measures: Technical measures include the use of secure equipment. The Agency's IT systems 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. The Agency's Corporate Local Informatics Security Officer (C-LISO) has the role of ensuring the Agency is compliant with this decision, and the application of security measures recommend by DIGIT. Netcompany-Intrasoft applies all appropriate technical and organizational measures to ensure the safe processing of personal data and to prevent the accidental loss or destruction and unauthorized and / or illegal access to, use, modification or disclosure thereof. In assessing the appropriate level of security and in the process of selecting and implementing suitable technical and organizational measures, Netcompany-Intrasoft

	takes into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing, as well as the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed, and additionally, the risk of varying likelihood and severity for the rights and freedoms of natural persons.
14	**Information to data subjects / Privacy Statement**
	Data subjects will be informed about the processing of their data. This is done through the DPN at the communication with the NEOs and will be made available in the File section of the dedicated TEAMS channel for NEOs.

Part 2 - Compliance Check and Risk Screening

Compliance check (Articles 4 and 5)

1

Legal basis of the processing

Please indicate the applicable part of Article 5(1)(a)-(e) of the Regulation giving the legal basis to this processing:

☒ (a) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body,

- the “2022 annual work programme “Erasmus+”: the Union Programme for Education, Training, Youth and Sport on” on page 74:
- The Commission Implementing Decision 2021/173 establishing the European Education and Culture Executive Agency;
- Regulation (EU) 2021/817 of the European Parliament and of the Council of 20 May 2021 establishing Erasmus+: the Union Programme for education and training, youth and sport and repealing Regulation (EU) No 1288/2013
- The Commission Decision C(2021)951 and its annexes delegating powers to EACEA for the management of programmes in the MFF 2021-2027.

☒ (d) the data subject has given consent to the processing of his or her personal data for one or more specific purposes:

- Audio and video recording of events and other external communication purposes (pictures, testimonials etc), by activating camera or audio, by agreeing to be photographed, or by submitting their testimonials etc
- Photographs of Community members and organisers of Community events may be taken and published on the platform. Participants who do not want to be photographed will be distinguished from those who give their consent by receiving a specific badge.
- Submitting non mandatory personal data on MS Teams and on platforms of the contractor (Beyond (BeyondLive | Virtual Events Platform | Beyond Live | BeyondLiveX.com; B2match (Event Platform Built for Networking (b2match.com); Slido (Slido - Audience Interaction Made Easy); Aventri (https://www.aventri.com)

Article 10(2)(a): Explicit consent for processing of health-related data concerning participants to physical events (allergies, accessibility etc), by submitting voluntarily such data.

2

Detailed description of the Processing

We will collect personal data like names, email addresses for a network for National Erasmus Offices (NEOs). This information will be stored by the EACEA in order to be able to reach the NEOs and to establish a network among them.
It is foreseen to create a Microsoft TEAMs channel where communication with and among the NEOs can be established.
The contact information of individuals representing the NEOs will not be made public by EACEA but used only for networking within that group, for exchanging relevant information and documents and for meetings with the EACEA, other Commission services, EU Delegations, National Agencies, the Higher Education Reform Experts (HERES); SPHERE (the contractor managing the HERES) and the contractors for ENFPs and the Erasmus+ International Students and Alumni Networks. It is foreseen that the NEOs and the above-mentioned institutions and individuals will meet at networking events online and in person.
A specific TEAMs channel will be also put in place for the NEO.
The individual NEOs can be reached via the Erasmus+ webpage managed exclusively by DG EAC (National Erasmus+ Offices | Erasmus+ (europa.eu)).

3	**Definition/scope of the Purpose(s) of the Processing**
	☒ **yes** ☐ **no** The collection and storage of contact details of NEOs is necessary to be able to contact the NEOs and to create a network among them. Moreover, for networking purposes it is necessary to connect the NEOs with the National Agencies and other stakeholders as outlined above. If information is also processed for further purposes, are you sure that these are compatible with the initial purpose(s)? ☐ **yes** ☒ **no.** Please explain: Personal data collected will not be used for further purposes.
4	**Data minimisation and proportionality**
	We collect and process personal data strictly necessary to establish and implement the network. Furthermore, the availability of email addresses and the mentioning of names are necessary so the NEOs can be contacted and the NEOs can contact each other and be contacted. No other personal data is collected.
5	**Data Accuracy**
	Name and contact details are collected directly from the person working for the NEOs who submit their details to EACEA. The NEOs will always be able to inform the EACEA about a change of contact details. Personal data can be rectified at any stage. Moreover, the EU Delegation or the competent national authority can inform the EACEA at any time about a change.
6	**Storage and Security**
	STORAGE: All information is stored in a restricted folder on the Drive accessible to specific staff members in EACEA & EAC who are authorised to access it on a need-to-know basis. **SECURITY:**[1] File location and access to the functional mailbox are restricted. Indicate the date or period of the beginning of the processing operations: 01.01.2022 Is the processing in question connected with the use of telecommunications networks? ☒ yes ☐ no Is the processing carried out in cooperation with an entity external to the Agency (co-controller)? ☐ yes ☒ no Is the processing carried out by an entity external to the Agency (processor)? ☐ yes ☒ no **1) Physical security/Organisational measures** Please specify measures taken: File location and access to the functional mailbox are restricted. All data in electronic format (e-mails, documents, uploaded batches of data etc.) are stored either

[1] Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality'). (Art 4(1)(f)).

on the servers of the European Commission or of its contractors. Their operations abide by the Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission.

The Commission's contractors are bound by a specific contractual clause for any processing operations of personal data on behalf of the European Commission, and by the confidentiality obligations deriving from the Regulation.

In order to protect personal data, the European Commission has put in place a number of technical and organisational measures. Technical measures include appropriate actions to address online security, risk of data loss, alteration of data or unauthorised access, taking into consideration the risk presented by the processing and the nature of the personal data being processed. Organisational measures include restricting access to the personal data solely to authorised persons with a legitimate need to know for the purposes of this processing operation. The access to personal data is protected by the management of the access rights which are strictly limited to specific users, as explained below.

Access rights are covered by robust authentication services and strict permissions management (including EU Login, network passwords, 2-factor authentication etc). The IT systems and tools are kept updated and monitored by DIGIT to ensure the security of the processing of personal data.

Sensitive information must be clearly labelled as such and encrypted using strong encryption keys to minimize the risk of exposure.

2) IT security
(Examples: coding control, undue removal or transmission of data, passwords, encrypted directories, backup, audit trails for data processing and communication, etc.)

Are data stored in an encoded format?
☒ yes □ no

Does the (software or service) development process respect established standards for secure software development?[2]
☒ yes □ no

In case the software (or cloud service) is configurable, do configuration options take into account basic security standards?[3]
☒ yes □ no

If third party components are in use (e.g. code libraries), do they correspond to established industry standards for security?[4]
□ yes □ no > N/A
The Agency’s data is hosted on infrastructure owned or managed by DG DIGIT (and hence meets DG DIGIT's security standards). This includes the following measures to ensure security:

1. Antivirus updates & scheduled scanning

2. Mirroring & Back-up between server rooms in two different sites

3. Secured Server Rooms & IT Stocks

4. Locks on material

[2] If the processing is based on corporate IT tools (eg: Ares, Sysper), please tick YES.

[3] As above.

[4] As above.

5. Business Continuity Plan (BCP) & Disaster Recovery Plan (DRP) with annual test.

When documents are stored on restricted corporate tools/servers/drives, they are protected in the following manner:

1. Web Filter – Blocks access to risky sites
2. Spam Filter – Scans all incoming mail to prevent malware download
3. Firewall & Proxy– Secures the network
4. Network Monitor – Detect suspicious traffic
5. Vulnerability Scanning – Detect known weakness
6. Software updates – Fix known risks
7. Daily backups take place

3) Staff security

Access to data through a restricted folder on the O-Drive and a Functional Mailbox to which only selected colleagues have access.
Upon entry to the building badges are checked and unauthorized personnel is not allowed to enter the building. EACEA staff is bound by a confidentiality rule (contractual obligation/requirement) and access to personal data follows a need-to-know basis.

Contractor:
Netcompany-Intrasoft applies all appropriate technical and organizational measures to ensure the safe processing of personal data and to prevent the accidental loss or destruction and unauthorized and / or illegal access to, use, modification or disclosure thereof. In assessing the appropriate level of security and in the process of selecting and implementing suitable technical and organizational measures, Netcompany-Intrasoft takes into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing, as well as the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed, and additionally, the risk of varying likelihood and severity for the rights and freedoms of natural persons.

7	**Retention time**
	EACEA will keep the data in the restricted U-Drive and in Microsoft TEAMS until either the individuals representing NEOs wants to delete the information, until the national authority will change especially the legal representative, or until the NEO network ceases to exist (at least, until the end of the current MFF 2021-2027). The data needs to be stored for this duration because the EACEA needs to have means to be able to reach out to the NEOs and to ensure that they can network with each other. " For health data (allergies, accessibility), EACEA will delete them as soon as they are not needed after the concerned event.
8	**Transparency: How do you inform people about the processing?**

	Data subjects will be informed about the processing of their data. This is done through the DPN at the communication with the NEOs and will be made available in the File section of the dedicated TEAMS channel for NEOs. .
9	**Access and other rights of persons whose data you process**
	No information about the identity of the NEOs will be provided to third parties, apart from the recipients mentioned under point 12. NEOs have the right to: - Request to access the personal data we have on them; - Request a rectification of their personal data or make the corrections themselves in their profiles; - Request the erasure of their personal data; - Request the restriction of the processing of their personal data; - Object to the processing of their personal data; - Request for their data to be transferred to another organization in commonly used machine-readable standard format (data portability); - Withdraw their consent at any time. To exercise their rights (access, rectify, request the restriction, object the processing of your data) they can contact the Data Controller at the email address above. As this processing of your personal data is based on point of Article 5(1)(a) of the data protection regulation, please note that you have the right to object to processing of your personal data on grounds relating to your particular situation under the provisions of Article 23 of the data protection regulation. In addition, as this processing of your personal data is based on your consent [Article 5(1)(d) or Article 10(2)(a) of the data protection regulation], please note that you can withdraw it at any time, and this will have effect from the moment of your retraction. The processing based on your consent before its withdrawal will remain lawful. However, rights to access, rectify or erase may be restricted by the Controller on a case-by-case basis: this is done in line with the Decision of the Steering Committee on internal rules concerning restrictions of certain rights of data subjects in relation to the processing of personal data in the framework of activities carried out by the Education, Audio-visual and Culture Executive Agency (OJ L 92, 17.3.2021, p. 6–14 - link). This decision was adopted pursuant to Article 25 of the Regulation. Restriction shall be proportionate to what is strictly necessary for the purpose of the processing. In order to grant or not the data subjects rights, the Agency will carry out a case-by-case assessment of each individual request and give the reasons underlying its decision for restriction.

Part 3 Risk screening (threshold assessment / criteria)
Article 39 Regulation

1	**Is the processing operation included in the EDPS' positive list?**
	☐ yes ☒ no If yes, please detail:… If the kind of processing operation you want to implement is included on the EDPS' positive list (see Annex for information and guideline) you do not need to fill-in Part 3.2 but you should proceed with the Data Protection Impact Assessment (DPIA).
Does the processing involve any of the following?	

2	**A systematic and extensive evaluation of personal aspects or scoring, including profiling and predicting**
	☐ yes ☒ no If yes, please detail *Examples: bank screening transactions in accordance with applicable law to detect possibly fraudulent transactions; profiling staff members based on all their transactions in EA's case management system with automatic reassignment of tasks.* *Counter example: standard staff appraisal interviews; 360° evaluations for helping staff members development plans.*
3	**Automated decision-making with legal or similar significant effect: processing that aims at taking decisions on data subjects**
	☐ yes ☒ no If yes, please detail *Example: automated staff appraisal ("if you're in the lowest 10% of the team for the number of cases dealt with, you'll receive an 'unsatisfactory' in your appraisal, no discussion"). Counter example: a news site showing articles in an order based on past visits of the user*
4	**Systematic monitoring**: processing used to observe, monitor or control data subjects, especially in publicly accessible spaces.
	☐ yes ☒ no If yes, please detail *This may cover video-surveillance but also other monitoring, e.g. of staff internet use. Examples: covert CCTV, data loss prevention tools breaking SSL encryption.* *Counter example: open CCTV of garage entry not covering public space.*
5	**Sensitive data**: data revealing ethnic or racial origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, biometric data for identification purposes, data concerning health or sex life or sexual orientation, criminal convictions or offences and related security measures or otherwise considered sensitive.
	☒ yes ☐ no Limited dietary needs/requirements for catering at onsite events submitted voluntarily
6	**Data processed on a large scale**, whether based on number of people concerned and/or amount of data processed about each of them and/or permanence and/or geographical coverage.
	☐ yes ☒ no If yes, please detail *Examples: European databases on disease surveillance.* *Counter example: internal EA phone directory*
7	Datasets matched or combined from **different data processing operations** performed for different purposes and/or by different data controllers in a way that would exceed the reasonable expectations of the data subject.
	☐ yes ☒ no If yes, please detail *Examples: covertly cross-checking access control logs, computer logs and flexitime declarations to detect absenteeism.*

	Counter example: transfer of personal file following a change of institution
8	Data concerning **vulnerable data subjects**: situations where an imbalance in the relationship between the position of the data subject and the controller can be identified.
	☐ yes ☒ no If yes, please detail *Examples: children, asylum seekers.* *Counter example: EA staff are not a priori considered as vulnerable vis-à-vis their employer concerning standard procedures laid down by the Staff Regulations*
9	**Innovative** use or applying **technological** or **organisational solutions** that can involve novel forms of data collection and usage.
	☐ yes ☒ no If yes, please detail Indeed, the personal and social consequences of the deployment of a new technology may be unknown. *Examples: machine learning, connected cars, social media screening of applicants for posts.* *Counter examples: biometric access control using fingerprints.*
10	**Preventing data subjects** from exercising a **right** or using a **service** or a **contract**.
	☐ yes ☒ no If yes, please detail *The individuals representing the NEOs have to sign a declaration of absence of conflict of interest in which they state that they are personally not part of any Erasmus+ project or project application.*
11	**Transfer of personal data outside EU without legislative basis**
	☐ yes ☒ no If yes, please detail (see point 12 of Part 1)

Part 4 – Conclusion

1	**Number of "Yes" ticked above**
	1
2	**Assessment**
	The processing does not entail specific risks in light of the EDPS list and criteria above related to the DPIA. The processing of personal data related to health as mentioned above is very limited.
3	**DPO Advice** (to be filled in by DPO)**:**
	No DPIA is required. The DPO agrees with the assessment of the controller above.
4	**Is a DPIA triggered?** (to be filled in by Controller)
	☐ yes ☒ no **Please explain:…**

Part 5 – For the DPO

1	Is the processing of personal data on a positive or negative list of the EDPS (art. 39(4) or art. 39(5))? ☐ yes ☒ no
2	Has a DPIA already been carried out in the context of the adoption of a legal act (art 39(10))? ☐ yes ☒ no
3	Is it on the list of the EC for prior consultation (art 40(4))? ☐ yes ☒ no

Part 6 - Linked documentation

1	**(where applicable) Links to threshold assessment and DPIA** **[not applicable**
2	**Where are your information security measures documented?**
3	**Other linked documentation** N/A

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[5];
- 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;
- Standard access control systems (non-biometric);

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

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