2024

Data management plan and IPR management

D1.3 DATA MANAGEMENT PLAN AND IPR MANAGEMENT

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them

Contents

1. IPR management processes for the MCEU project

The success of the project depends on achieving unanimous agreement among all participating partners regarding explicit guidelines concerning the ownership of intellectual property (IP), access rights to both Background and Foreground IP for project execution and safeguarding intellectual property rights (IPR) and confidential information before the project commences. These matters are extensively outlined in the Consortium Agreement, which involves all project partners. The IPR Management process describes how all partners, as described in the "Agreement of Joint Data Control" for the MCEU project, will handle data, documents, and products created through the MCEU project.

This document applies to all partners mentioned in the "Agreement of Joint Data Control." It builds on information from the Grant Agreement (pages 24-26), where the IPR rules regarding this project are described in detail. The purpose of the Consortium Agreement is to establish a legal framework for the project, providing clear regulations for issues within the consortium related to IP Ownership, Confidential Information, Open-Source issues, Standard contributions, and Access Rights to Background and Foreground IP for the duration of the project and any other matters of the consortium's interest.

As described in the Consortium Agreement, each Partner owns the project results that they have solely produced. If two or more Project Partners have jointly produced project results, ownership shall belong to all Partners jointly. The Partners do not assume responsibility for the other Partners' exploitation of project results generated wholly or partially by the Partners. The partners must give each other, and the other participants, access to the background identified as needed for implementing the action, subject to any specific rules in Annex 5 in the grant agreement.

'Background' means any data, know-how, or information — whatever its form or nature (tangible or intangible), including any rights such as intellectual property rights — that is: (a) held by the beneficiaries before they acceded to the Agreement and (b) needed to implement the action or exploit the results. If background is subject to the rights of a third party, the beneficiary concerned must ensure that it is able to comply with its obligations under the Agreement.

In case certain results are identified to be essential for the future business opportunities of the involved partners, necessary steps will be taken to protect such results accordingly. The patenting and other protective measure procedures will proceed along the regulations set forth in the Consortium Agreement.

All partners in the program are aware of the "Open access requirements for educational material" that apply to the MCEU project as described below:

"*Erasmus+ promotes open access to project outputs to support learning, teaching, training, and youth work. In particular, Erasmus+ beneficiaries are obliged to make any educational resources and tools which are produced in the context of projects supported by the Programme – documents, media, software, or other materials freely available to the public under an open license. The materials should be easily accessible and retrievable without cost or limitations, and the open license must allow the public to use, reuse, adapt, and share the resource. Such materials are known as 'Open Educational Resources' (OER). To achieve this aim, the resources should be uploaded in an editable digital form and on a suitable and openly accessible platform. While Erasmus+ encourages beneficiaries to apply the most open licenses, beneficiaries may choose licenses that impose some limitations, e.g., restrict commercial use by others, or commit others to apply the same license on derivative works, provided that this is appropriate to the nature of the project and to the type of material in question, and that it still allows*

the public to use, reuse, adapt, and share the resource. The open access requirement is obligatory and is without prejudice to the intellectual property rights of the grant beneficiaries."[1]

2. Agreement on Joint Data Control = Data management plan

See the next 18 pages.

[1] https://erasmus-plus.ec.europa.eu/programme-guide/part-a/important-characteristics-of-the-erasmus-programme

Agreement on Joint Data Control

between

Data controller 1

PROFESSIONSHOJSKOLEN UNIVERSITY COLLEGE NORDJYLLAND (UCN),

PIC No: 950017710

Selma Lagerlofs vej 2

9000 Aalborg

Denmark

and

Data controller 2

DIPLOMASAFE APS (DIPLOMASAFE APS)

PIC No: 894639149

Dronningens Tvaergade 4 A, 1

1302 Copenhagen

Denmark

and

Data controller 3

HOSPITALITY CONNECTION BARCELONA SL (Hosco),

PIC No: 907049620

Carrer Roger De Flor, 221

08025 Barcelona

Spain

and

Data controller 4

ESTUR ESCUELA DE TURISMO DE SANT POL DE MAR, S.L. (C.G.R. Sant Pol)

PIC No: 884322714

Calle Riera Vaquer 22

08395 Sant Pol De Mar (Barcelona)

Spain

and

Data controller 5

IDAN FRAEDSLUSETUR EHF (IDAN),

PIC No: 948899300,

Vatnagardar 20

104 Reykjavik

Iceland

and

Data controller 6

SAMTOK FERDATHJONUSTUNNAR (SAF)

PIC No: 880759031,

Borgartuni 35

105 Reykjavik

Iceland

and

Data controller 7

NALCO EUROPE B.V. (Nalco),

PIC No: 883020392

Oude Rhijnhofweg 17

2342 bb Oegstgeest

Netherlands

and

Data controller 8

ACCESS ADVISORS

PIC No: 886422764

Rue Saint-Pierre 63

1000 Brussels

Belgium

March 2024

1. Joint controllers

1.1. This Agreement sets out the respective responsibilities of Data controller 1 to Data controller 8 relating to:

All Partners in the project have a joined data controller responsibility regarding the collection of data from the three surveys made under the MCEU project. Hosco will have the responsibility of creating the surveys and collecting the data from them, while UCN, Hosco, IDAN and Sant Pol are responsible for distributing the data.

Hosco will have the responsibility of processing the raw data while the aggregated data will be available for all project partners.

1.2. According to Article 26 of the General Data Protection Regulation (the GDPR), two or more data controllers become joint controllers when they jointly determine the purposes and means of personal data processing.

If the data protection responsibility is joint, the joint data controllers shall determine in a transparent manner their respective responsibilities for compliance with the obligations under the GDPR, in particular in regards to the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14 of the GDPR by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject.

According to Article 26(2) of the GDPR, the arrangement shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subject.
The essence of the arrangement shall be made available to the data subject.

Irrespective of the terms of the arrangement, the data subject may exercise his or her rights under the GDPR in respect of and towards each of the controllers.

Similarly, the respective responsibilities of the parties to this Agreement shall not prevent the supervisory authority from taking measures against Data controller 1 and/or Data controller 2.

1.3. Data controller 1 to data controller 8 agree that joint data protection responsibilities exist relating to before mentioned activities in 1.1. In determining the existence of such joint responsibilities, the following factor(s) was/were decisive:

- One of the main objects of MCEU is making surveys and collecting personal data from companies and employees that operate in Spain, Iceland and Denmark. It is the partners joint responsibility to ensure that this data is treated correctly, regarding the GDPR regulation.

- All parties have in collaboration decided which test, surveys and evaluation to be used during the MCEU-project. The "agreement of joint data Control" is therefore also made to secure that all parties follow the requirements aligned in this agreement together with the rules and guidelines described in the articles that the agreement refers to.

1.4. This Agreement is drawn up in order to enable Data controller 1 and Data controller 2 to comply with the requirements of Article 26 of the GDPR on joint data controller responsibilities. This Agreement sets out the respective responsibilities of Data controller 1 and Data controller 2 for compliance with the obligations under the GDPR, in particular regarding to the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14.

2. General responsibilities

2.1. **UCN:** Responsibility and disclosure obligation in relation to the dissemination of surveys. In addition, UCN is responsible for events, which involve disclosure obligations, obtaining consent, and recording participation. As the coordinator, UCN is responsible for the operation and maintenance of the website, ensuring that information is accurate and up-to-date. If a newsletter is created, UCN is also responsible for managing email lists and withdrawing consent. UCN also provides the Microsoft Teams platform, which involves a SharePoint solution with maintained rights management and access permissions on the platform.

UCN will have the main responsibility regarding GDPR for the deliverables under Workpackage 1:

UCN will only process ordinary personal data such as name, gender, address, phone number, date of birth, email address, etc., and not personal data that requires a higher level of protection, such as CPR numbers, criminal records, etc.

2.2. **Hosco:** As described in 1.1, Hosco will be responsible for processing the raw data.

Hosco will have the main responsibility regarding GDPR for the deliverables under Workpackage 2:

Hosco will only process ordinary personal data such as name, gender, address, phone number, date of birth, email address, employment status, country of residence, etc., and not personal data that requires a higher level of protection, such as CPR numbers, criminal records, etc.

2.3. **Nalco** (Lobster Ink) will be responsible for WP3: Development of micro-credential courses.

Nalco will only process ordinary personal data such as name, gender, address, phone number, date of birth, email address, etc., and not personal data that requires a higher level of protection, such as CPR numbers, criminal records, etc.

2.4. **Diplomasafe:** will be responsible for WP4: Credential issuing online platform and WP6: Communication dissemination, and sustainability.

Diplomasafe will only process ordinary personal data such as name, gender, address, phone number, date of birth, email address, etc., and not personal data that requires a higher level of protection, such as CPR numbers, criminal records, etc.

2.5. **IDAN:** will be responsible for WP5: Piloting micro credential courses.

IDAN will only process ordinary personal data such as name, gender, address, phone number, date of birth, email address, etc., and not personal data that requires a higher level of protection, such as CPR numbers, criminal records, etc.

2.6. **Sant Pol:** Will not be responsible for a workpackage but will have a role in regarding data collecting conducting eg. Surveys.

Sant Pol: will only process ordinary personal data such as name, gender, address, phone number, date of birth, email address, etc., and not personal data that requires a higher level of protection, such as CPR numbers, criminal records, etc.

2.7. SAF: Will not be responsible for a workpackage but will have a role in regarding datacollecting conducting eg. Surveys.

SAF: will only process ordinary personal data such as name, gender, address, phone number, date of birth, email address, etc., and not personal data that requires a higher level of protection, such as CPR numbers, criminal records, etc.

2.8. **IDAN:** Will not be responsible for a workpackage but will have a role in regarding data collecting conducting eg. Surveys.

IDAN: will only process ordinary personal data such as name, gender, address, phone number, date of birth, email address, etc., and not personal data that requires a higher level of protection, such as CPR numbers, criminal records, etc.

2.9. **Access Advisors:** Will not be responsible for a workpackage but will have a role in regarding data collecting conducting eg. Surveys.

Access Advisors: will only process ordinary personal data such as name, gender, address, phone number, date of birth, email address, etc., and not personal data that requires a higher level of protection, such as CPR numbers, criminal records, etc.

3. Principles and legal basis underlying processing activities

3.1. All partners are responsible for the existence of a legally valid basis for processing activities and for providing documentary evidence of it, e.g. to the supervisory authority.

As mentioned in 2.1-2.8 each partner is responsible for their respective activities entailing data acquisition, processing and documentation in order to provide for an external supervisory authority in matters of documentary purposes.

3.2. Data controller 1 and Data controller 2 shall each be responsible for complying with the principles underlying personal data processing as applicable to each party's responsibilities as set out in this Agreement.

4. The rights of the data subject

4.1. All parties shall be responsible for protecting the rights of the data subject by complying with the following provisions of the GDPR:

- the obligation to provide information at the time of collection of personal data from the data subject,
- the obligation to provide information if personal data is not collected from the data subject,
- the data subject's right of access,
- the data subject's right to rectification,
- the data subject's right to erasure (right to be forgotten),
- the data subject's right to restriction of processing,
- the obligation to provide information relating to rectification or erasure of personal data or the restriction of processing,
- the data subject's right to data portability (except in the exercise of official authority) and
- the data subject's right to object to processing.

4.2. If a Data controller (ex. 1) receives a request or enquiry from a data subject about matters under the responsibility of another Data controller (ex. 2), cf. above, the request shall be forwarded to the respective Data controller (ex. 2) as soon as possible.

4.3. The Parties shall be responsible for assisting each other to the relevant and necessary extent for the fulfilment by all Parties of their obligations toward the data subject.

4.4. Each partner is represented in the MCEU project with a GDPR representative, who is lifting a coordinating function in regard to upholding each partners local responsibilities regarding GDPR.

5. Security of processing and documentation of compliance with the GDPR

5.1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, all

parties shall be responsible for implementing appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the GDPR. Where necessary, those measures shall be reviewed and updated. (Article 24 of the GDPR). This could for example mean that] all parties should draft procedures for the handling of security breaches, for the handling of requests for access, or for compliance with the obligation to provide information.

5.2. Where proportionate in relation to processing activities, the measures taken by all parties shall include the implementation of appropriate data protection policies.

5.3. all parties shall be responsible for observing the provisions on data protection by design and data protection by default as set out in Article 25 of the GDPR.

5.4. all parties shall be responsible for observing Article 32 of the GDPR on security of processing. This implies that while taking into account the actual technical standard, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, all parties shall implement appropriate technical and organisational measures to ensure a level of security appropriate to those risks.

For this reason, all parties shall carry out (and be able to document) a risk assessment and subsequently take measures to reduce the identified risks.

6. The use of data processors and sub-processors

6.1. all parties shall not be entitled to use data processors and/or any sub-processors in relation to the joint data processing activities, without involving the Project Management Team beforehand.

6.2. In the event of the use of data processors and/or sub-processors, all parties shall be responsible for complying with the requirements of Article 28 of the GDPR all parties shall subsequently be obliged to, inter alia,:

- use only processors providing appropriate safeguards to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subject.

- ensure the existence of a valid data processing agreement between all parties and the data processor, and

- ensure the existence of a valid sub-processing agreement between the data processor and any sub-processor.

6.3. On request, all parties shall be made aware of whether the information is being processed by data processors and, if applicable, sub-processors of the other parties.

6.4. If the information is being processed by data processors and any sub-processors, the Parties shall be informed, upon request, of the content of the agreements between the Parties and the data processor/sub-processor.

7. Records of processing activities

7.1. All Parties shall be responsible for complying with Article 30 of the GDPR on records of processing activities. This implies that all parties shall maintain a record of the processing activities under their joint data responsibility.

7.2. All parties shall inform each other of the contents of the above-mentioned record.

7.3. On the basis of the contents of each other's record, each party shall prepare their own record of the processing activities under the agreement.

8. Notification of a personal data breach to the supervisory authority

8.1. All parties shall be responsible for complying with Article 33 of the GDPR on notification of a personal data breach to the supervisory authority.

9. Communication of a personal data breach to the data subject

9.1. All parties shall be responsible for complying with Article 34 of the GDPR on communication of a personal data breach to the data subject.

10. Data protection impact assessment and prior consultation

10.1. All parties shall be responsible for complying with the requirement of Article 35 of the GDPR on data protection impact assessment. This implies that where a type of processing, in particular one using new technologies, and taking into account the nature, scope,

context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, all parties shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

10.2. All parties shall also observe the requirement of Article 36 of the GDPR on prior consultation of the supervisory authority, where relevant.

11. Transfers of personal data to third countries or international organisations

11.1. Jointly, the Parties can decide that personal data may be transferred to third countries or international organisations.

11.2. All Parties shall be responsible for observing the requirements of Chapter V of the GDPR in the event that personal data is transferred to third countries or international organisations.

12. Complaints

12.1. Each party shall be responsible for processing any complaints from data subjects in the event that the complaints concern infringement of the GDPR for which that Party is responsible pursuant to this Agreement.

12.2. If either of the parties receives a complaint that should rightfully be dealt with by the other party, the complaint must be forwarded to that Data controller as soon as possible.

12.3. If either of the Parties receives a complaint of which part of the complaint should rightfully be dealt with by the other Party, that part of the complaint must be forwarded to the Party for processing as soon as possible.

12.4. When a complaint or parts of a complaint are transmitted to the other Party, the data subject must be notified of the essence of this Agreement.

13. Notification of the other Party

13.1. The Parties shall inform each other of essential matters that impact on the joint data processing activities and this Agreement.

14. Effective date and termination

14.1. This Agreement shall come into effect upon signature by all parties.

14.2. This Agreement shall remain in force for as long as the personal data concerned is being processed or until the Agreement is replaced by a new agreement that sets out the parties' responsibilities relating to the processing activities.

15. Signatures

On behalf of **UCN**

Name: THOMAS FISKE NIELSEN

Position: Head of Act Learn

Date: 22/3-24

On behalf of **DIPLOMASAFE**

_____

Name: _____

Position: _____

Date: _____

On behalf of **HOSCO**

_____

Name: _____

Position: _____

Date: _____

On behalf of **SANT POL**

_____

Name: _____

Position: _____

Date: _____

On behalf of **IDAN**

_____

Name: _____

Position: _____

Date: _____

On behalf of **SAF**

_____

Name: _____

Position: _____

Date: _____

On behalf of **NALCO**

_____

Name: _____

Position: _____

Date: _____

On behalf of **ACCESS ADVISORS**

_____

Name: _____

Position: _____

Date: _____


MCEU