

# DELIVERABLE No. 1.11

## Data Protection Laws implemented

Version as of 20/11/2023

<b>Acronym</b>	EDUC
<b>Full Name</b>	European Digital UniverCity – The bridging alliance
<b>Grant Agreement No.</b>	101089535
<b>Programme</b>	ERASMUS-EDU-2022-EUR-UNIV-1
<b>Instrument</b>	European Universities Initiative
<b>Start date</b>	01/01/2023
<b>Duration</b>	48 months
<b>Deliverable No.</b>	1.11
<b>Document name</b>	D1.11 Data Protection Laws implemented
<b>Work Package</b>	WP 1 EDUC Governance, Management and Coordination
<b>Task</b>	Task 1.5 Ensure data security and privacy
<b>Dissemination Level</b>	public
<b>Contractual Submission Date</b>	M12
<b>Actual Submission Date</b>	M14
<b>Name responsible Institution (task lead)</b>	UJI
<b>Contact</b>	<a href="mailto:info@educ-alliance.eu">info@educ-alliance.eu</a>
<b>Abstract</b>	This data joint controller agreement constitutes the legally binding contract among EDUC partners that states the rights and obligations of each party concerning the protection of personal data as processed by the EDUC solutions and services.
<b>Keywords</b>	Personal data; data subject; processing; data sharing; joint controller; data protection; agreement; GDPR



Université  
de Rennes



MUNI



UN  
University of  
South-Eastern



Université  
Paris Nanterre

## Agreement on the Joint Control of Personal Data pursuant to Art. 26 GDPR

**Between (as Data Controller 1)**

### **Universitat Jaume I**

represented by its Rector, Prof. Eva Alcón Soler

represented in turn by its Vice-Rector for International Relations, Prof. Eva Camacho Cuenca,  
Avinguda de Vicent Sos Baynat, s/n,  
12006 Castelló de la Plana (Castelló) – Spain

**And (as Data Controller 2)**

### **University of Cagliari**

represented by its Rector, Prof. Francesco Mola  
Via Università, 40  
09124 Cagliari - Italy

represented in turn by its Vice-Rector for International Affairs, Prof. Alessandra Carucci  
Direzione per la Ricerca ed il Territorio  
Via San Giorgio, 12  
09124 Cagliari - Italy

**And (as Data Controller 3)**

### **Masaryk University**

represented by its Rector, Prof. Martin Bareš

represented in turn by the Vice-Rector for Internationalisation, Petr Suchý, Ph.D.  
Žerotínovo nám. 617/9  
60177 Brno - Czech Republic

**And (as Data Controller 4)**

### **University Paris Nanterre**

represented by its President, Prof. Philippe Gervais-Lambony  
200 avenue de la République  
92001 Nanterre Cedex - France





Université  
de Rennes



MUNI



University of  
South-Eastern



Université  
Paris Nanterre

**And (as Data Controller 5)**

**University of Pécs**

represented by its Rector, Prof. Attila Miseta

represented in turn by its Chancellor, István Decsi,

Vasvári Pál Utca 4

7622 Pécs - Hungary

**And (as Data Controller 6)**

**University of Rennes**

represented by its President, Prof. David Alis

Bâtiment 1A

263 Av. Général Leclerc

35042 RENNES Cedex

CS 74205 - France

**And (as Data Controller 7)**

**University of South-Eastern Norway**

represented by its Rector, Prof. Petter Aasen

represented in turn by its Vice-Rector for Education, Ingvild Marheim Larsen

Postboks 4

3199 Borre - Norway

**And (as Data Controller 8)**

**University of Potsdam**

represented by its President, Prof. Oliver Günther

represented by its Chancellor, Mr Hendrik Woithe

Zentrum für Informationstechnologie und Medienmanagement (ZIM)

Am Neuen Palais 10

14469 Potsdam - Germany



## Section 1. Introduction, Scope, Definitions

- (1) This contract governs the rights and obligations of the Parties as joint data controllers (hereinafter referred to as the "Parties" or "Data Controller 1" [or 2, 3, 4, 5, 6, 7 or 8]).
- (2) This contract applies to activities performed for the purpose of fulfilling the EDUC contract that involve the processing of personal data by employees of the Parties or processors engaged by them.
- (3) The Parties have jointly determined the aims and purposes of the processing activities described in more detail below, together with the technologies and methods (means) to be used to achieve them. Therefore, they are joint controllers under the terms of Art. 4 (7) GDPR.
- (4) The terms used in this contract are to be understood according to their definition in the GDPR.
- (5) The term "Subject", or "Data Subject", is used in this context as an identified or identifiable natural person: an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (as defined in GDPR Art. 4.1)
- (6) "Adminstrating Controller": The person who coordinates each service, manages the technology used and is responsible for the processing of the data involved.
- (7) "Processing Controllers": The persons who process the data and are responsible for the user data collected in the services by the associated universities.

## Section 2. Subject and Duration of the Processing of Personal Data

### (1) Subject

The subject of this Agreement is the processing of the personal data described in more detail below: The European Digital UniverCity (EDUC) is an alliance formed by eight European universities to foster collaboration in the areas of teaching, research, innovation and the third mission. Participating universities are:

- University of Cagliari (Italy)
- Masaryk University (Czech Republic)
- University Paris Nanterre (France)
- University of Pécs (Hungary)
- University of Potsdam (Germany)
- University of Rennes (France)
- University of South-Eastern Norway (Norway)
- Universitat Jaume I (Spain)

In addition to the above, all aspects of the EDUC project are covered in terms of infrastructure, data, procedures and services for education through the competences of the universities in the consortium.

## **(2) Duration**

The Agreement is valid until the end of the EDUC project (31 December 2026). The Parties will review it for modifications or renewal for future periods before it expires. The Agreement can be terminated by any of the Parties by giving at least three months' notice prior to the end of the running semester that ends the latest among the partner universities. Termination by one Party does not terminate the contractual relationship between the remaining Parties.

## **(3) Special Right of Termination**

- (a) Each Party can terminate this Agreement at any time without complying with a notice period ("extraordinary termination") if another Party commits a serious violation of data protection regulations or the stipulations of this Agreement. A serious violation will be deemed to exist in particular if one Party has largely failed to fulfil the obligations defined in this Agreement, particularly in the case of the agreed technical and organisational measures.
- (b) For insubstantial violations by one Party, the other Parties must set a reasonable deadline for remedying the defect. If no remedy is undertaken in good time, the Parties are also entitled to extraordinary termination.
- (c) In case of extraordinary termination, the Party found to be in breach of the contract and initiating the termination is to reimburse the other Party for all the costs that are incurred due to the premature termination of the Main Contract or of this contract.

## **Section 3. Specification of the Contents of the Agreement**

### **(1) Type and purpose of the intended data processing**

A detailed description of the subject of the contract as regards the type and purpose of the joint data processing: The types of processing are collection, recording, organisation, structuring, storage, adaptation or alteration, commenting or correcting, retrieval, use, dissemination or otherwise making available, restriction, erasure or destruction. The purpose of data processing is the provision of the shared systems and services within the framework of the cross-border European learning and teaching project (EDUC). Those systems and services are better explained in the annex created for each service, and the annex should be an integral part of this Agreement.

### **(2) Type of data**

The object of the processing of personal data are the following data types and categories (list and description of the data categories)

- ☒ Personal data regarding master's degrees
- ☒ Communication data (e.g. telephone number, email address)
- ☒ User registration data
- ☒ Access log
- ☒ Planning and control data
- ☒ Content data (e.g. teaching materials, commentaries, examinations, chats, uploaded materials)
- ☒ Academic data
- ☒ Job-related data
- ☒ Financial and accounting data

### (3) Categories of data subjects

The categories of the data subjects comprise:

- ☒ Students
- ☒ Doctoral candidates
- ☒ Examination candidates
- ☒ External users of higher education institutions
- ☒ Employees (e.g. teachers, administrative staff)

## Section 4. Obligations of the Data Controllers

### (1) Ensuring compliance with the legal provisions

Each Party must ensure compliance with the legal provisions, particularly as regards the legality of the data processing activities they conduct themselves. All Parties are equally responsible for complying with the legal provisions, particularly as regards the legality of the data processing activities they conduct together.

- (2) The Parties must take all necessary technical and organisational measures to ensure that the rights of the data subjects, particularly those pursuant to Chapter III GDPR, are safeguarded at all times within the statutory time limits.
- (3) The main office of Data Controller 1 is considered the headquarters and serves as a reference to determine the supervisory authority responsible.
- (4) Data Controller 1 is committed to supervising the data protection information required in accordance with Art. 13 and 14 of the GDPR and necessary for each service, and also to providing it to the other Data Controllers.
- (5) The point of contact for exercising rights as data subjects resulting from Art. 15 to 21 GDPR is, for general technical data, the Adminstrating Controller running each platform or Data Controllers of the respective university of affiliation of the teacher(s) for the courses or modules taught. Related to this is the obligation to make the information available to data subjects upon request, pursuant to Art. 15 GDPR, and to handle processing requests in compliance with Art. 16 to 21 GDPR. All Processing Controllers must cooperate, if necessary, to facilitate the exercise of rights.

- (6) If data subjects pursuant to Art. 26 subsection 3 GDPR assert a claim to information or other rights resulting from Chapter III of the GDPR towards the other Data Controller(s), the request will be forwarded to the respective Data Controllers named in subsection (5).
- (7) Data Controller 1 commits to providing data subjects with the obligatory information pursuant to Art. 26 subsection 2 GDPR. The essentials of this Agreement, including the respective actual functions and the relationships of the joint Data Controllers, must be made available to the data subjects in a transparent way.
- (8) All Parties commit to designing the internal organisation in their respective areas of responsibility such that they fulfil the special requirements of data protection. Each Party will take technical and organisational measures that fulfil the requirements of the relevant data protection provisions in order to adequately secure the data against abuse and loss.
- (9) Any security breach that significantly affects the personal data subject under this Agreement must be communicated, without undue delay, to Controller 1 by sending an email to [dpo@educalliance.eu](mailto:dpo@educalliance.eu) so that the appropriate steps can be taken to comply with Art. 33 and 34 of the GDPR.

## Section 5. General Obligations when Processing

- (1) The Parties declare in a legally binding manner that all persons engaged for the purposes of data processing are committed to confidentiality before beginning their work, or that they are subject to an appropriate statutory or confidentiality obligation anchored in a collective agreement.
- (2) If professional secrets protected by laws and regulations are affected by the processing, all Parties declare in a legally binding manner that all the persons engaged for data processing were bound to confidentiality pursuant to laws and regulations before beginning their work. All persons engaged for data processing were, in addition, informed that the commitment to confidentiality continues to exist after terminating and leaving their work.
- (3) Furthermore, all persons are to be bound as regards the obligation to maintain the business and operating secrets of the Parties, and before beginning processing are to be reminded of laws and regulations and the consequences associated with a violation.
- (4) **"Principles relating to processing"**. Each and every joint controller must implement efficient technical and organisational measures to ensure that data processing is in accordance with Art. 5 of the GDPR, which states that personal data must be:
  - (a) **"Lawfulness, fairness and transparency"**: Processed in a lawful, fair and transparent manner in relation to the data subject.
  - (b) **"Purpose limitation"**: collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes; in accordance with Art. 89(1), further processing of personal data for archiving purposes in the public interest, scientific and

historical research purposes or statistical purposes will not be considered incompatible with the initial purposes;

- (c) **"Data minimisation"**: Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
  - (d) **"Accuracy"**: Accurate and, where necessary, kept up to date; all reasonable steps must be taken to ensure that personal data that are inaccurate in relation to the purposes for which they are processed are erased or rectified without delay;
  - (e) **"Storage time limitation"**: kept in a form which allows identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be kept for longer periods provided that they are processed exclusively for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Art. 89(1), without prejudice to the application of appropriate technical and organisational measures required by this Regulation in order to protect the rights and freedoms of the data subject;
  - (f) **"Integrity and confidentiality"**: Processed in such a way as to ensure appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, by implementing appropriate technical or organisational measures ("integrity and confidentiality").
  - (g) **"Proactive accountability"**: Ability to demonstrate compliance with the principles relating to processing.
- (5) Administrating Controllers must comply with the obligation to inform data subjects in the platforms or services they manage in accordance with Art. 13 and 14 of the GDPR in the forms set out in Art. 12 of the GDPR.

Although not exclusive or limitative in nature, information regarding the processing of data must be provided to data subjects:

- (a) Prior to the collection and processing of their data
  - (b) If the technology permits, the information must be provided in a double layer: the first containing the basic information and an additional layer with complementary information.
  - (c) Forms (printed or electronic), information sheets, clauses, pop-up systems, posters and any other means of providing information on data processing may be used.
  - (d) It must be possible to reliably demonstrate that the information has been provided.
  - (e) Where the processing requires the express consent of the data subject, it must be in accordance with Art. 7 of the GDPR.
  - (f) In the case of minors, the provisions of Art. 8 of the GDPR should be taken into account.
  - (g) Where recourse is made to obtaining the data subject's electronic signature, legally valid digital signature procedures and systems must be used.
- (6) **"Management of requests for the exercise of rights"**. All co-responsible parties must implement technical and organisational measures to deal with requests to exercise rights within a maximum of 30 days. All requests to exercise rights must be dealt with in accordance with Art. 4(5) and reported to [dpo@educalliance.eu](mailto:dpo@educalliance.eu).

(7) **“Register of Processing Activities”**. Any personal data processing activity carried out jointly by the joint controllers must be previously defined, analysed and approved by consensus and recorded in the joint Data Processing Activities Register and contain at least the headings set out in Art. 30 of the GDPR.

(8) **“Privacy by default and by design”**. Any product or service developed, administered and/or contracted by any of the joint controllers must comply with the provisions of Art. 25 of the GDPR regarding the implementation of privacy by default and by design.

(9) **“Impact Assessments”**. Any intention to process personal data that poses a high risk to the rights and freedoms of individuals must first be subject to the execution of an Impact Assessment and a copy must be sent to all those jointly responsible for the processing.

(10) **“International data transfers”**. International data transfers outside the European Economic Area (EEA) are not permitted. Where, due to force majeure, it is necessary to carry out international data transfers outside the EEA, these must be previously documented, communicated and approved by all the joint controllers and must guarantee the preservation of the rights and freedoms of data subjects, as well as compliance with the provisions of Chapter V of the GDPR.

(11) **“Contact with data subjects”**. The following email address has been established as a point of contact with data subjects: [dpo@educalliance.eu](mailto:dpo@educalliance.eu).

However, data subjects may choose to contact any of the co-responsible parties at their convenience.

(12) **“Security measures”**. In accordance with Art. 32 of the GDPR, taking into account the current status of the issue, the costs of implementation, and the nature, scope, context and purposes of the processing, as well as the risks of varying likelihood and severity to the rights and freedoms of natural persons, all joint controllers must implement technical and organisational measures to ensure a level appropriate to the risk. Such measures must include, where appropriate and among others, the following:

- (a) the pseudonymisation and encryption of personal data.
- (b) the ability to ensure the continued confidentiality, integrity, availability and resilience of processing systems and services.
- (c) The ability to restore availability and access to personal data in a timely manner in the event of a physical or technical incident.
- (d) A process of regular verification, evaluation and assessment of the effectiveness of technical and organisational measures to ensure the security of the processing.

In assessing the adequacy of the level of security, each co-responsible controller should in particular take into account the risks presented by the data processing, especially as a result of the accidental or unlawful destruction, loss or alteration of personal data transmitted, stored or otherwise processed, or unauthorised disclosure of or access to such data.

Adherence to an approved code of conduct within the meaning of Art. 40 of the GDPR or to an approved certification mechanism within the meaning of Art. 42 of the GDPR may serve as an element to demonstrate compliance with the security requirements.

Each joint controller must take steps to ensure that any person acting under their authority who has access to personal data may process such data only on the instructions of the joint controller and on the basis agreed to in this Data Processing Agreement.

## **Section 6. Rectification, Restriction of Processing, Erasure and Return of Data Storage Media**

- (1) During the term of this Agreement, any significant changes one Party intends to make within the scope of its responsibilities regarding rectification, erasure or restriction of data processed under this contract will only be possible following consultation with the other Parties. For any significant changes, if no reply is received from the other Parties within 60 days, it may be assumed that the other Parties agree to the proposed measure, ensuring operational efficiency while maintaining data protection standards. To encourage consistency, consultation for minor changes is recommended but not compulsory under the contract.
- (2) If destruction of data storage media and other materials is to be undertaken during ongoing processing, the respective Data Controller will ensure such destruction is performed in a manner compliant with data protection regulations.

## **Section 7. Contracted Data Processing**

- (1) Where a joint controller intends to use a third party to outsource services, such a relationship must be regulated by a Commissioning Agreement in accordance with Art. 28 of the GDPR. The contracting controller must ensure that the service provider has in place means to ensure full compliance with the GDPR and the fundamental rights and freedoms of data subjects. The other Parties must be informed at least 30 days before the conclusion of the contract.
- (2) Each Party has the right to object to the engagement of a specific processor in the event of good cause, provided that such objection is communicated within 30 days from the date of receiving the initial notification. Failure to raise an objection within this timeframe will be deemed as acceptance of the processor engagement.
- (3) Processors must provide their contractual services within the European Union (EU) or the European Economic Area (EEA). If a provision of services is carried out by a processor in a third country, all Parties must have given their consent to this.
- (4) The respective processor must, in order to ensure fulfilment of the obligations resulting from this Agreement, be contractually bound by the Party engaging the processor.
- (5) Each processor must ensure that, upon deploying sub-contractors, the obligations arising from

this Agreement are also fulfilled by the sub-contractors.

- (6) Every processor must have appointed a data protection officer. The contact details of the data protection officer must be made available to all parties.

## Section 8. Procedure regarding future changes in the conditions, new services and new Data Controllers - "Parties"

- (1) Any modification that affects the Joint Processing that, in turn, affects the Joint Controllers will be supplemented by the corresponding Appendix that sets out all the details of the processing, as well as the responsibilities and obligations of each of the Parties in terms of data protection.
- (2) Any attached addendum will be subject to any and all the provisions of this Agreement, and will form an integral part thereof.
- (3) Each of the Appendices must be accepted and signed by all parties.

## Section 9. Other

- (1) The Parties' data protection officers are listed in Appendix 1 to this Agreement.
- (2) If individual stipulations of this Agreement should prove to be, completely or in part, ineffective or unfeasible or to become ineffective or unfeasible as a consequence of changes in legislation after conclusion of the contract, the remaining contractual stipulations and the effectiveness of the contract overall remain unaffected by this.
- (3) The effective and executable stipulation that is as close as possible to the meaning and purpose of the invalid stipulation should supersede the ineffective or unfeasible stipulation.

If the contract proves to have any omissions, the stipulations that correspond to the meaning and purpose of the contract apply as agreed and as would have been agreed on had they been taken into account.

## Signatures

### Controller 1: Universitat Jaume I

Represented by its Rector, Prof. Eva Alcón Soler  
represented in turn by its Vice-Rector for International Relations,  
Prof. Eva Camacho Cuena, Relations, by virtue of the powers delegated  
by the Rector by means of the Resolution  
dated 24 May 2022 (DOGV of 27 May)





Controller 2: **University of Cagliari**

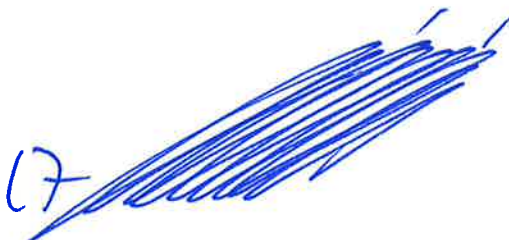
Represented by its Rector, Prof. Francesco Mola  
represented in turn by its Vice-Rector for International Affairs,  
Prof. Alessandra Carucci by virtue of the powers delegated  
with Rector's Decree n° 427 of 7<sup>th</sup> May 2021





Controller 3: **Masaryk University**

Represented by its Rector, Prof. Martin Bareš  
Žerotínovo nám. 617/9  
60177 Brno - Czech Republic

(7) 



Controller 4: **University Paris Nanterre**

Represented by its President

Philippe Gervais-Lambony





Controller 5: University of Pécs (5 signatures)

University of Pécs

represented by its Rector, Prof. Attila Miseta



represented in turn by its Chancellor, István Decsi,



Vasvári Pál Utca 4  
7622 Pécs - Hungary



Controller 6: University of Rennes



16/03/2024

Le Président de l'Université de Rennes

David ALIS



**Controller 7: University of South-Eastern Norway**

represented by its Rector, Prof. Pia Cecilie Bing-Jonsson  
represented in turn by its Vice-Rector for Education, Ingvild Marheim Larsen  
Postboks 4, 3199 Borre – Norway

Place and date

Drammen, 20.02.24

Signature and stamp

*Pia C. Bing-Jonsson*



Controller 8: University of Potsdam

*Handwritten signature of Mr Hendrik Woithe*

Mr Hendrik Woithe, Chancellor  
Der Kanzler  
Am Neuen Palais 10  
14469 Potsdam

*Handwritten date and place: 2.4.24 Potsdam*

Date, Place

Stamp

*Handwritten signature of Prof. Oliver Günther*

Prof. Oliver Günther, President

*Handwritten date and place: April 9, 2024, Potsdam*

Date, Place

Stamp

UNIVERSITÄT POTSDAM  
Der Präsident  
Am Neuen Palais 10  
14469 Potsdam

Appendix 1 - Data Protection Officers of the Data Controllers





Université  
de Rennes



MUNI



University of  
South-Eastern



Université  
Paris Nanterre

Currently appointed as the internal data protection officer at Data Controller 1:

**Universitat Jaume I**

Edifici Rectorat i Serveis Centrals. Campus de Riu Sec.

Castelló de la Plana (Castelló) - Spain

Email: [dpd@uji.es](mailto:dpd@uji.es)

Currently appointed as the internal data protection officer at Data Controller 2:

**University of Cagliari**

via Università, 40

09124 Cagliari - Italy

Email: [dpo@unica.it](mailto:dpo@unica.it)

Currently appointed as the internal data protection officer at Data Controller 3:

**Masaryk University**

Žerotínovo nám. 617/9

60177 Brno - Czech Republic

Email: [poverenec@muni.cz](mailto:poverenec@muni.cz)

Currently appointed as the internal data protection officer at Data Controller 4:

**University Paris Nanterre**

Service des Affaires Juridiques et Institutionnelles (SAJI)

Bâtiment Pierre Grappin

200 avenue de la République

92001 Nanterre Cedex - France

Email: [dpo@liste.parisnanterre.fr](mailto:dpo@liste.parisnanterre.fr)

Currently appointed as the internal data protection officer at Data Controller 5:

**University of Pécs**

Vasvári P. u. 4.

7622 Pécs - Hungary

Email: [adatvedelem@pte.hu](mailto:adatvedelem@pte.hu)

Currently appointed as the internal data protection officer at Data Controller 6:

**University of Rennes**

Monsieur le Président de l'Université de Rennes

A l'attention de la déléguée à la protection des données

Direction des Affaires Juridiques et Institutionnelles (DAJI)

Co-funded by the  
Erasmus+ Programme  
of the European Union



European  
Digital  
UniverCity

[www.educalliance.eu](http://www.educalliance.eu)



**Université  
de Rennes**



**MUNI**



**USN**  
University of  
South-Eastern



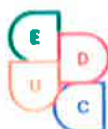
**Université  
Paris Nanterre**

Bâtiment 1A  
263 av Général Leclerc  
35042 RENNES CEDEX  
CS 74205 - France  
Email: [dpo@univ-rennes.fr](mailto:dpo@univ-rennes.fr)

Currently appointed as the internal data protection officer at Data Controller 7:  
**University of South-Eastern Norway**  
Postboks 43199 Borre - Norway  
Email: [Postmottak@usn.no](mailto:Postmottak@usn.no)

Currently appointed as the internal data protection officer at Data Controller 8:  
**University of Potsdam**  
Am Neuen Palais 10  
14469 Potsdam - Germany  
Email: [datenschutz@uni-potsdam.de](mailto:datenschutz@uni-potsdam.de)

Co-funded by the  
Erasmus+ Programme  
of the European Union



**European  
Digital  
UniverCity**

[www.educalliance.eu](http://www.educalliance.eu)

## Appendix 2 – Data Protection Regulation for Virtual Learning Environment

### 1. Purpose of processing

The central e-learning platform "Virtual Learning Environment" under the URL <https://learning.educalliance.eu/> is established in order to promote and execute electronically supported learning ("e-learning") among the participating universities and to make it accessible on a uniform platform.

### 2. Personal data processed

With registration in the Virtual Learning Environment, the following personal data will be processed:

- (1) User account (corresponds to the respective university account or a guest account).
- (2) Surname and first name.
- (3) User's email address at their home university or email address of the guest account.
- (4) Name of home organisation (university).
- (5) Log data, e.g. IP-addresses and at what time users access which parts of the course offerings.
- (6) Session cookie.
- (7) User data: Course application data, content, contributions and activities of the user in Moodle.

### 3. Specific Provisions on Data Processing

Currently, the entire Moodle infrastructure is hosted and managed by the University of Potsdam, but in the future the Controllers have agreed to move the entire Moodle infrastructure and administration to the Universitat Jaume I. So, the specific provisions on Data Processing are:

For as long as the infrastructure is hosted and managed by the University of Potsdam:

- (1) **"Administering Controller"**: Controller 8 (University of Potsdam) will be responsible for processing personal data for purposes 1 to 7.
- (2) **"Processors-Controllers"**. Controllers 1, 2, 3, 4, 5, 6, and 7 will be responsible for processing personal data for purposes 1 to 4 and 7.

For as long as the infrastructure is hosted and managed by the Universitat Jaume I:

- (1) **"Administering Controller"**: Controller 1 (Universitat Jaume I) will be responsible for processing personal data for purposes 1 to 7.
- (2) **"Processors-Controllers"**. Controllers 2, 3, 4, 5, 6, 7 and 8 will be responsible for processing personal data for purposes 1 to 4 and 7.

## 4. Data source

---

The personal data processed in the Virtual Learning Environment are provided by the interested party or one of the participating universities.

## 5. Lawfulness of processing

---

- (1) **Students.** The legal basis for the processing of student's personal data is Art. 6 para. 1 sentence 1 lit. e GDPR. This provision allows the processing of personal data for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. It has to be complemented by a legal basis set out in Union law or in the law of the Member States from which the specific tasks to be carried out are derived. These complementing provisions differ for the processing performed by each of the joint controllers:
- (a) **Universitat Jaume I:** Organic Law 2/2023, of 22 March, on the University System. Art. 2 describes the services that Spanish universities must offer and Art. 3 grants them.
  - (b) **University of Cagliari:** ROYAL DECREE n. 1592, of 31 August 1933. Approval of the consolidated version of higher education laws. Art. 33 of the Italian Constitution, which provides that universities have the right to adopt autonomous systems within the limits established by the laws of the State. Law 9 May 1989, n. 168. Establishment of the Ministry of Universities and Scientific and Technological Research. University Statute issued on 9 July 2019 n. 765.
  - (c) **Masaryk University:** Sec. 88 of Higher Education Act N. 111/1998 Coll. According to this provision, higher education institutions in the Czech Republic must process the personal data of its students and graduates for the state registry and transfer them to the Ministry of Education, Youth and Health. Section 16 of the Czech Act on Personal Data Processing – No.110/2019 Coll. deals with processing of personal data for the purpose of scientific or historical research or for statistical purposes.
  - (d) **University Paris-Nanterre:** Law number 78-17, of 6 January 1978, on information technology, files and civil liberties. According to this law, the legal basis for data processing is the 1st Title, Chap. 1, Art. 5, lit. 5. This provision allows personal data to be processed for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
  - (e) **University of Pécs:** Art. 18 and Annex 3, point I. of Act CCIV of 2011 on higher education regulates the data processing operations at the universities, including some

rules regarding the students. Art. 18 lists the possible data processing purposes, the relevant ones being “to ensure the proper operation of the university” and “to grant the rights and ensure obligations of the students”. The appendices list the potential categories of personal data processed, including – among others – the students’ identification data (name, time and place of birth, etc.), contact data (contact address, telephone number, etc.), data about their education (courses, exams, credits, foreign studies), etc.

- (f) **University of Rennes:** Law number 78-17, of 6 January 1978, on information technology, files and civil liberties. According to this law, the legal basis for data processing is the 1st Title, Chap. 1, Art. 5, lit. 5. This provision allows personal data to be processed for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
  - (g) **University of South-Eastern Norway:** Act relating to universities and university colleges LOV-2005-04-01-15 §4–15(1). The educational institution may process personal data regarding an applicant, student or doctoral candidate when the purpose of the processing is to safeguard the rights of the data subject, or to fulfil the institution's tasks and duties under the Act relating to universities and university colleges.
  - (h) **University of Potsdam:** Sec. 14 Para. 9 Brandenburg Higher Education Act (BbgHG). According to this provision, institutions of higher education in the state of Brandenburg may process the personal data of applicants, students, doctoral students, examination candidates and external users of higher education facilities that are required for the participation in courses, examinations and the use of higher education facilities, among others.
- (2) **Employees.** The legal basis for processing employees’ personal data stems from Art. 88 GDPR. This provision opens up the possibility for Member States to create specific rules for the processing of personal data in employment contexts through legislation or collective agreements, including for the purpose of the performance of employment contracts. These specific rules differ for the processing performed by each of the joint controllers:
- (a) **Universitat Jaume I:** Royal Legislative Decree 5/2015, of October 30, by which the Consolidated Version of the Law of the Basic Statute of Public Employees is approved. Law 4/2021, of April 16, on the Valencian Civil Service. Royal Legislative Decree 2/2015, of 23 October, by which the revised text of the Workers' Statute Law is approved. Organic Law 2/2023, of March 22, of the University System.
  - (b) **University of Cagliari:** Requirements relating to the processing of special categories of data in labour relations (aut. gen. no. 1/2016) referred to in Provision [9124510] pursuant to Art. 21, paragraph 1 of Legislative Decree no. 10 August 2018, no. 101.
  - (c) **Masaryk University:** In accordance with Act No. 110/2019 Coll., the Personal Data Processing Act, it is permissible to process personal data of employees based on the

employment contract concluded with them, which includes facilitation of educational courses and management of personal information concerning employees' professional activities within the institution.

- (d) **University Paris-Nanterre:** Law number 78-17, of 6 January 1978, on information technology, files and civil liberties. According to this law, the legal basis for data processing is the 1st Title, Chap. 1, Art. 5, lit. 5. This provision allows personal data to be processed for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
  - (e) **University of Pécs:** Art. 10-11/A. of the Act I of 2012 on the Labour Code provides some more detailed rules on processing employees' data. Art. 18 and Annex 3, point I. of Act CCIV of 2011 on higher education regulates the data processing operations at universities, including some rules regarding the employees. Art. 18 lists the possible data processing purposes, the relevant ones are "to ensure the proper operation of the university" and "to carry out obligations and exercise rights regarding employment of teachers, researchers and other employees". The appendices list the potential categories of personal data processed, including – among others – the employees' identification data (name, time and place of birth, etc.), contact data (contact address), employment data, etc.
  - (f) **University of Rennes:** Law number 78-17, of 6 January 1978, on information technology, files and civil liberties. According to this law, the legal basis for data processing is the 1st Title, Chap. 1, Art. 5, lit. 5. This provision allows personal data to be processed for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
  - (g) **University of South-Eastern Norway:** The Act relating to the working environment, working hours and employment protection, etc. (Working Environment Act) § 14-5 and § 14-6 on the employment contract, seen together with the act relating to universities and university colleges LOV-2005-04-01-15 § 1- 3 (a to g on the activities of the institutions), provides a legal basis for the processing of employees' personal data for the purpose of conducting courses, etc.
  - (h) **University of Potsdam:** Sec. 26 Para. 1 Brandenburg Data Protection Act (BbgDSG). According to this provision, public entities in the state of Brandenburg, such as the University of Potsdam, may process employees' personal data in connection with, among other things, the performance of the respective employment contract. This includes processing the personal data of the state universities' employees for the purpose of conducting courses.
- (3) **Cookies.** The processing of personal log data and personal data in connection with the storage of session cookies on personal devices is carried out on the basis of the aforementioned provisions.

- (a) For as long as the infrastructure is hosted and managed by the University of Potsdam, the storage of session cookies on the personal device itself is based on Section 25 para. 2 No. 2 German Telecommunications Telemedia Data Protection Act (TTDSG).
  - (b) For as long as the infrastructure is hosted and managed by the Universitat Jaume I, the storage of session cookies on the personal device itself is based on Art. 22 (2), Spanish Law 34/2002, of 11 July, on information society services and electronic commerce (LSSICE).
- (4) **Consent.** Insofar as the data processed by the Virtual Learning Environment is not necessary for students' participation in courses or the performance of employment contracts by employees, the processing is carried out on the basis of consent pursuant to Art. 6 para. 1 sentence 1 lit. a GDPR. This specifically applies to optional account data, which can be added by users by editing their profile. These data include: user pictures, additional names, interests, optional contact data and date of birth. The consent is given conclusively by providing the data.

## 6. Withdrawal of consent

Data subjects have the right to withdraw their consent at any time and without giving any reason. The withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal. Data subjects can delete their optional user data or voluntary entries in the user profile at any time by themselves.

## 7. Duration of data processing

The data in the user profile (registration data) are stored until the user profile is deleted. The data from participation in courses (user data) are stored until the course is deleted. Log data is deleted 365 days after the end of the usage process. Session cookies are deleted when the user logs out, when their Virtual Learning Environment session ends after a long period of inactivity, or when they end their browser session.

## 8. Recipients of subjects' data

- (1) Only the staff responsible for the administration and management of the central e-learning platform will have access to all the data stored in the system, including the log files. They may process this data solely to ensure the operation of the Virtual Learning Environment. The evaluation of user data for statistical purposes may only be carried out in an anonymous form by the persons named in sentence 1. Data is anonymised by deleting the personally identifiable information.

- (2) Teachers will only have access to the activities, contributions and data provided by their course participants insofar as these are generally accessible in the Virtual Learning Environment or are accessible within the course.

## 9. Data Processors

---

For as long as the infrastructure is hosted and managed by the University of Potsdam, there is no third-party processing the data under the authority of the controller.

For as long as the infrastructure is hosted and managed by the Universitat Jaume I, the whole IT structure is hosted in AWS (Amazon Web Services).

## 10. Data security

---

For as long as the infrastructure is hosted and managed by the University of Potsdam, the safety measures include, at least:

(1) Organisational measures

- Access management for sites and equipment
- Incident management
- Backup and recovery concept
- Training of user awareness

(2) Technical measures

- Use of firewalls and malware protection
- Creation of regular backups
- Encryption of storage
- Identity and access control
- Monitoring of user login and activities
- Security maintenance and updates

For as long as the infrastructure is hosted and managed by the Universitat Jaume I, the safety measures are:

- (1) The security measures established in the Spanish National Security Framework (ENS), at medium level, and specified in Annex 2 of Royal Decree 311/2022, of 3 May, which regulates the National Security Framework.
- (2) To view this, please visit the following link: [https://administracionelectronica.gob.es/dam/jcr:eb23ff83-ebdb-487e-abd2-8654f837794f/RD\\_311-2022\\_of-3\\_May\\_ENS.pdf](https://administracionelectronica.gob.es/dam/jcr:eb23ff83-ebdb-487e-abd2-8654f837794f/RD_311-2022_of-3_May_ENS.pdf).

## Appendix 3 – Data Protection Regulation for Course Catalogue

### 1. Purpose of processing

The "Course Catalogue" platform available at the URL <https://courses.educalliance.eu/> is established for the discovery and enrolment of courses in the catalogue offered among the participating universities and to make it accessible on a uniform platform.

### 2. Personal data processed

With registration on the Course Catalogue, the following personal data will be processed:

- (1) User account (corresponds to the respective university account or a guest account).
- (2) Surname and first name.
- (3) User's email address at their home university or the email address of the guest account.
- (4) Name of home organisation (university).
- (5) Log data, e.g. IP addresses and at what time users access which parts of the course offerings.
- (6) Session cookie.
- (7) User data: Course application data, content, contributions and activities of the user in the Virtual Learning Environment, enrolment data.

### 3. Specific Provisions on Data Processing

Currently, the entire Virtual Learning Environment infrastructure is hosted and managed by the University of Potsdam, but in the future the Controllers have agreed to move the entire Virtual Learning Environment infrastructure and administration to the Universitat Jaume I. So, the specific provisions on Data Processing are:

For as long as the infrastructure is hosted and managed by the University of Potsdam:

- (1) **"Adminstrating Controller"**: Controller 8 (University of Potsdam) will be responsible for processing personal data for purposes 1 to 7.
- (2) **"Processors-Controllers"**. Controllers 1, 2, 3, 4, 5, 6, and 7 will be responsible for processing personal data for purposes 1 to 4 and 7.

For as long as the infrastructure is hosted and managed by the Universitat Jaume I:

- (3) **"Adminstrating Controller"**: Controller 1 (Universitat Jaume I) will be responsible for processing personal data for purposes 1 to 7.

- (4) **“Processors-Controllers”**. Controllers 2, 3, 4, 5, 6, 7 and 8 will be responsible for processing personal data for purposes 1 to 4 and 7.

## 4. Data source

---

The personal data processed in the Courses Catalogue are provided by the interested party or one of the participating universities.

## 5. Lawfulness of processing

---

- (1) **Students**. The legal basis for the processing of students’ personal data is Art. 6 para. 1 sentence 1 lit. e GDPR. This provision allows personal data to be processed for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. It has to be complemented by a legal basis in Union law or in the law of the Member States from which the specific tasks to be carried out are derived. These complementing provisions differ for the processing performed by each of the joint controllers:
- (a) **Universitat Jaume I**: Organic Law 2/2023, of 22 March, on the University System. Art. 2 describes the services that Universities must offer and Art. 3 grants it.
  - (b) **University of Cagliari**: ROYAL DECREE n. 1592, of 31 August 1933. Approval of the consolidated version of higher education laws. Art. 33 of the Italian Constitution which provides that universities have the right to adopt autonomous systems within the limits established by the laws of the State. Law 9 May 1989, n. 168. Establishment of the Ministry of Universities and Scientific and Technological Research. University Statute issued on 9 July 2019 n. 765.
  - (c) **Masaryk University**: Sec. 88 of Higher Education Act N. 111/1998 Coll. According to this provision, higher education institutions in the Czech Republic must process the personal data of its students and graduates for the state registry and transfer them to the Ministry of Education, Youth and Health. Section 16 of the Czech Act on Personal Data Processing – No.110/2019 Coll. deals with processing of personal data for the purpose of scientific or historical research or for statistical purposes.
  - (d) **University Paris-Nanterre**: Law number 78-17, of 6 January 1978, on information technology, files and civil liberties. According to this law, the legal basis for data processing is the 1st Title, Chap. 1, Art. 5, lit. 5. This provision allows personal data to be processed for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
  - (e) **University of Pécs**: Art. 18 and Annex 3, point I. of Act CCIV of 2011 on higher education regulates the data processing operations at the universities, including some

rules regarding the students. Art. 18 lists the possible data processing purposes; the relevant ones being “to ensure the proper operation of the university” and “to grant the rights and ensure obligations of the students”. The appendices list the potential categories of personal data processed, including – among others – the students’ identification data (name, time and place of birth, etc.), contact data (contact address, telephone number, etc.), data about their education (courses, exams, credits, foreign studies), etc.

- (f) **University of Rennes:** Law number 78-17 of 6 January 1978 on information technology, files and civil liberties. According to this law, the legal basis for data processing is the 1st Title, Chap. 1, Art. 5, lit. 5. This provision allows personal data to be processed for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
  - (g) **University of South-Eastern Norway:** Act relating to universities and university colleges LOV-2005-04-01-15 §4–15(1). The educational institution may process personal data regarding an applicant, student or doctoral candidate when the purpose of the processing is to safeguard the rights of the data subject, or to fulfil the institution's tasks and duties under the Act relating to universities and university colleges.
  - (h) **University of Potsdam:** Sec. 14 Para. 9 Brandenburg Higher Education Act (BbgHG). According to this provision institutions of higher education in the state of Brandenburg may process the personal data of applicants, students, doctoral students, examination candidates and external users of higher education facilities that are required for the participation in courses, examinations and the use of higher education facilities, among others.
- (2) **Employees.** The legal basis for processing employees’ personal data stems from Art. 88 GDPR. This provision opens up the possibility for Member States to create specific rules for the processing of personal data in employment contexts through legislation or collective agreements, including for the purpose of the performance of employment contracts. These specific rules differ for the processing performed by each of the joint controllers:
- (a) **Universitat Jaume I:** Royal Legislative Decree 5/2015, of October 30, by which the Consolidated Version of the Law of the Basic Statute of Public Employees is approved. Law 4/2021, of April 16, on the Valencian Civil Service. Royal Legislative Decree 2/2015, of 23 October, by which the revised text of the Workers' Statute Law is approved. Organic Law 2/2023, of March 22, of the University System.
  - (b) **University of Cagliari:** Requirements relating to the processing of special categories of data in labour relations (aut. gen. no. 1/2016) referred to in Provision [9124510] pursuant to Art. 21, paragraph 1 of Legislative Decree no. 10 August 2018, no. 101.
  - (c) **Masaryk University:** In accordance with Act No. 110/2019 Coll., the Personal Data Processing Act, it is permissible to process personal data of employees based on the

employment contract concluded with them, which includes facilitation of educational courses and management of personal information concerning employees' professional activities within the institution.

- (d) **University Paris-Nanterre:** Law number 78-17, of 6 January 1978, on information technology, files and civil liberties. According to this law, the legal basis for data processing is the 1st Title, Chap. 1, Art. 5, lit. 5. This provision allows personal data to be processed for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
- (e) **University of Pécs:** Art. 10-11/A. of the Act I of 2012 on the Labour Code provides some more detailed rules on processing employees' data. Art. 18 and Annex 3, point I. of Act CCIV of 2011 on higher education regulates the data processing operations at universities, including some rules regarding the employees. Art. 18 lists the possible data processing purposes, the relevant ones are "to ensure the proper operation of the university" and "to carry out obligations and exercise rights regarding employment of teachers, researchers and other employees". The appendices list the potential categories of personal data processed, including – among others – the employees' identification data (name, time and place of birth, etc.), contact data (contact address), employment data, etc.
- (f) **University of Rennes:** Law number 78-17, of 6 January 1978, on information technology, files and civil liberties. According to this law, the legal basis for data processing is the 1st Title, Chap. 1, Art. 5, lit. 5. This provision allows personal data to be processed for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
- (g) **University of South-Eastern Norway:** The Act relating to the working environment, working hours and employment protection, etc. (Working Environment Act) § 14-5 and § 14-6 on the employment contract, seen together with the act relating to universities and university colleges LOV-2005-04-01-15 § 1- 3 (a to g on the activities of the institutions), provides a legal basis for the processing of employees' personal data for the purpose of conducting courses, etc.
- (h) **University of Potsdam:** Sec. 26 Para. 1 Brandenburg Data Protection Act (BbgDSG). According to this provision, public entities in the state of Brandenburg, such as the University of Potsdam, may process employees' personal data in connection with, among other things, the performance of the respective employment contract. This includes processing the personal data of the state universities' employees for the purpose of conducting courses.

- (3) **Cookies.** The processing of personal log data and personal data in connection with the storage of session cookies on personal devices is carried out on the basis of the aforementioned provisions.

- (a) For as long as the infrastructure is hosted and managed by the University of Potsdam, the storage of session cookies on the personal device itself is based on Section 25 para. 2 No. 2 German Telecommunications Telemedia Data Protection Act (TTDSG)
- (b) For as long as the infrastructure is hosted and managed by the Universitat Jaume I, the storage of session cookies on the personal device itself is based on Art. 22 (2), Spanish Law 34/2002, of 11 July, on information society services and electronic commerce (LSSICE).

## 6. Duration of data processing

---

The data in the user profile (registration data) are stored until the user profile is deleted. The data from participation in courses (user data) are stored until the course is deleted. Log data is deleted 365 days after the end of the usage process. Session cookies are deleted when the user logs out, when their Moodle session ends after a long period of inactivity, or when they end their browser session.

## 7. Recipients of subjects' data

---

- (1) Only the staff responsible for the administration and management of the central e-learning platform "Course Catalogue" will have access to all the data stored in the system, including the log files. They may process this data solely to ensure the operation of the Course Catalogue. The evaluation of user data for statistical purposes may only be carried out in an anonymous form by the persons named in sentence 1. Data is anonymised by deleting the personally identifiable information.
- (2) Teachers will only have access to the activities, contributions and data provided by their course participants insofar as these are generally accessible in the Courses Catalogue or are accessible within the course.

## 8. Data Processors

---

For as long as the infrastructure is hosted and managed by the University of Potsdam, there is no third-party processing the data under the authority of the controller.

For as long as the infrastructure is hosted and managed by the Universitat Jaume I, the whole IT structure is hosted in AWS (Amazon Web Services).

## 9. Data security

---

For as long as the infrastructure is hosted and managed by the University of Potsdam, the safety measures include at least:

**(1) Organisational measures**

- Access management for sites and equipment
- Incident management
- Backup and recovery concept
- Training of user awareness

**(3) Technical measures**

- Use of firewalls and malware protection
- Creation of regular backups
- Encryption of storage
- Identity and access control
- Monitoring of user login and activities
- Security maintenance and updates

For as long as the infrastructure is hosted and managed by the Universitat Jaume I, the safety measures are:

- (1) The security measures established in the Spanish National Security Framework (ENS), at medium level, and specified in Annex 2 of Royal Decree 311/2022, of 3 May, which regulates the National Security Framework.
- (2) To view this, please visit the following link: [https://administracionelectronica.gob.es/dam/jcr:eb23ff83-ebdb-487e-abd2-8654f837794f/RD\\_311-2022\\_of-3\\_May\\_ENS.pdf](https://administracionelectronica.gob.es/dam/jcr:eb23ff83-ebdb-487e-abd2-8654f837794f/RD_311-2022_of-3_May_ENS.pdf).