Data Protection Policy of

Central European University
Private University – CEU GmbH

2021
Vienna, Austria

Contents

Overview of the Data Protection Policy

This Data Protection Policy (hereinafter the "Policy") was prepared and issued by Central European University Private University - CEU GmbH (hereinafter "CEU"), located in Quellenstrasse 51, 1100 Vienna, Austria, and registered with the Austrian Commercial Register under FN502313x, as **Data Controller** in order to comply with the applicable data privacy requirements, including specifically the EU General Data Protection Regulation (hereinafter: "GDPR")[1] and other applicable laws as stated in Annex 1 to this document (applicable law or data protection law).

At CEU we place great emphasis on the protection of personal data and compliance with applicable law. Therefore, by adopting this Policy, CEU seeks to ensure – among others – that:

1. it is clear about how personal data must be processed and what its expectations are for all those who process personal data on its behalf;
2. it complies with the data protection law and with good practice;
3. CEU's reputation is protected by ensuring the personal data entrusted to it is processed in accordance with Data Subjects' rights; and
4. CEU is protected from risks of personal data breaches and other breaches of data protection law.

Accountability

CEU is responsible for and must be able to demonstrate compliance with data protection principles and laws. CEU demonstrates compliance with the data protection principles by

- having implemented this Policy and other related policies;

- establishing procedures on documenting how personal data is handled and by producing required documentation such as Privacy Notices, Record of Processing Activities;

- keeping records on e.g. Personal Data Breaches;

- implementing a Privacy by Design principle and requesting for the completion of a Data Protection Impact Assessment (DPIA) where processing presents a high risk to the privacy of Data Subjects;

- appointing a suitably qualified DPO;

- training staff on compliance with data protection law; and

- regularly improving the privacy measures implemented at CEU and conducting periodic reviews and audits to assess compliance.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

The main terms used in this Policy are defined and explained in the glossary at the end of this Policy (Annex 2).

1. Scope and Policy Statement

1.1 CEU is committed to comply with all relevant EU and national laws, as applicable, in respect of using personal data, and the protection of the "rights and freedoms" of individuals whose information CEU collects and processes in accordance with the GDPR and other relevant data protection legislation (data protection law). When processing personal data, CEU is also obliged to fulfil individuals' reasonable expectations of their privacy by complying with applicable law.

1.2 CEU considers this Policy and other relevant policies of CEU (e.g. IT Policy), along with additional Privacy Notices and connected processes and procedures, the adequate framework and management tool for compliance with the GDPR.

1.3 This Policy applies to all of CEU's personal data processing activities regardless of the location where that personal data is stored (e.g. on an employee's own device) including those performed by potential staff, faculty and students (applicants), current/former staff, faculty and students, website users, contractors, partners, third party individuals and any other personal data that the organization processes from any source (collectively referred to in this Policy as "Data Subjects").

1.4 The Policy applies to all personal data managed by CEU regardless of the way it is collected, used, recorded, stored or destroyed, and irrespective of whether it is held in paper files or electronically.

1.5 This Policy applies to all Members of the CEU community. Compliance with data protection rules (including the applicable laws and this Policy) is the responsibility of all Members of the CEU Community who process personal data.

1.6 Any breach of this Policy shall constitute a misconduct under the applicable regulations of Austrian civil and employment laws and may also be considered a criminal offence, in which case the matter shall be reported as soon as possible to the appropriate authorities.

2. Responsibilities and roles under the GDPR

The Management of CEU and all those in managerial or supervisory roles at CEU are responsible for developing and encouraging good personal data handling practices and fostering data protection awareness within CEU.

All units, departments and centers acting as Data Owners shall designate a Data Steward who shall act as a liaison managing the data processing issues pertaining to the competence of the DPO and/or consulting the GDPR Team.

2.1 CEU responsibilities

As the Data Controller, CEU is responsible for establishing policies and procedures in order to comply with applicable data protection law.

2.2 Data Protection Officer responsibilities

CEU has appointed a Data Protection Officer (DPO) who is the key person for ensuring compliant operation regarding privacy issues. (mailto:privacy@ceu.edu)

The DPO is responsible for, among others:

(a) advising CEU and its staff of its obligations under GDPR;
(b) monitoring compliance with the GDPR and other relevant data protection law and the present Policy;
(c) monitoring and auditing activities ensuring GDPR compliance;
(d) providing advice when requested on data protection impact assessments (DPIA);
(d) cooperating with and acting as the contact point for the Authority;
(e) establish and run specific procedures such as the Subject Access Request Procedure;
(f) setting out training and awareness requirements in relation to specific roles of faculty and staff of CEU in general; and
(g) ensuring that all Members of the CEU Community are trained in the importance of collecting accurate data and maintaining it.

2.3 Members of CEU Community responsibilities acting on behalf of CEU

Members of CEU Community must ensure that:

(a) all personal data is kept securely, following IT guidelines on this matter (available on the IT intranet);
(b) no personal data is disclosed either verbally or in writing, accidentally or otherwise, to any unauthorized third party;
(c) personal data is kept in accordance with the corresponding Privacy Notice;
(d) any queries regarding data protection, including subject access requests (SAR) and complaints, are promptly directed to the DPO;
(e) any data protection breaches are swiftly brought to the attention of the DPO and that they support the DPO in resolving the breach;
(f) where there is uncertainty around a data protection matter, advice is sought from the GDPR Team and/or the DPO;
(g) personal data is only accessed by those who are in charge of dealing with them; and
(e) requests (including SAR) must be immediately forwarded to the DPO.

Where Members of the CEU Community are responsible for supervising students doing work which involves the processing of personal data (for example in study cases, research projects) on behalf of CEU, they must ensure that those students are aware of the requirements of the present Policy.

The Members of the CEU Community shall make sure that CEU employees, persons in a quasi-employee relationship with CEU ("Dienstnehmerähnliches Verhältnis" as stipulated in Section 51, subsection 3, number 2 and Section 4, subsection 4 of the Austrian General Social Insurance Act) and third-party service providers (Data Processors) will be contractually bound to observe data confidentiality during their contractual relationship and after termination according to this Policy.

2.4 Data Owners responsibilities

All Data Owners are responsible for ensuring that CEU staff within their area of responsibility comply with this Policy and should implement appropriate practices, processes, controls and training to ensure compliance.

Data Owners shall assure that any new process, project, procedure within their competence is implemented taking a data protection by design approach (e.g. keeping the amount of personal data to an absolute minimum, informing the individuals on the processing, finding the appropriate legal ground for processing, collecting valid consent and recording it, making data deletion/anonymization measures, keeping the data up-to-date, using access control and effective security (technical and organizational) measures to the data). For more on Privacy by Design please see section 12.

The Data Owner is responsible for contacting the GDPR Team and/or the DPO in case it seeks advice regarding the proper implementation of the Policy or other GDPR requirements including the preparation of Privacy Notice(s). In case the Data Owner disagrees with the proposal of the GDPR Team and/or the DPO, it is the Senior Leadership Team (SLT) who will decide on the privacy issues addressed to them by the Data Owner.

The Management of CEU expects that Data Owners:

- regularly establish objectives for data protection and privacy within their competence;
- properly document all aspects of the processing activities through a Privacy Notice, consent form, data deletion, withdrawal of consent, etc.;
- keep recorded the processing activities within their competence in the Record of Processing Activities (ROPA)/data map;
- ensure that personal data be deleted/destroyed after the end of the retention period;
– when selecting partners and/or any third parties working with or for the CEU who may have access to personal data, opt for service providers (Data Processors) whose commitment to privacy and the GDPR equals to the level of protection provided by CEU and/or GDPR standards;
- enter into a data processing agreement in accordance with Article 28 of the GDPR, which imposes on the third-party obligations no less onerous than those to which CEU is committed under applicable law.

2.5 Contractors, Short-Term and Voluntary Staff

CEU is responsible for the use of personal data made by anyone working on its behalf. Members of the CEU Community who are entitled to employ contractors, short term or voluntary staff must ensure that they are appropriately prepared for the planned data processing. In addition, it should be ensured that:

- a data processing agreement is signed with the contractor or short term / voluntary member of staff having access to personal data;
- all practical and reasonable steps are taken to ensure that contractors, short term or voluntary staff do not have access to any personal data beyond what is essential for the work to be carried out properly;
- any personal data collected or processed in the course of work undertaken for CEU is kept securely and confidentially; and
-all personal data is returned to CEU on completion of the work, including any copies that may have been made or alternatively, that the data is securely destroyed and the Member

of the CEU Community responsible for the cooperation receives notification in this regard from the contractor or short term / voluntary member of staff once this is done.

2.6 Members of the CEU Community responsibilities

Members of the CEU Community are responsible for:

(a) familiarising themselves with the Privacy Notice provided to them when they register with CEU or start employment or a contractual relationship with CEU;
(b) ensuring that their personal data provided to CEU is accurate and up to date; and
(c) notifying CEU of any changes in circumstances to enable personal records to be updated accordingly.

2.7 GDPR Team

The GDPR team is CEU's privacy expert knowledge center and helps Data Owners with advice and/or guidance on the proper implementation of the provisions of the GDPR and local legislations. The GDPR Team follows in its daily practice the approach of the present Policy to privacy and the mandatory requirements of applicable laws. The team shall support the drafting of Privacy Notices or other related documents as well as the development of all kinds of processing activities, including research activity with a strong focus on Privacy by Design, DPIA and precise application of data protection requirements

3. Data Protection Principles

All processing of personal data must be conducted in accordance with the data protection principles (hereafter "Principles") as set out in the GDPR. CEU's policies and procedures are designed to ensure compliance with the Principles.

1.1 Personal data must be processed **lawfully, fairly** and **transparently**

Lawfully – identify one lawful basis (legal ground) before you process personal data.

Processing shall be lawful only if and to the extent that at least one of the following applies:

a) the Data Subject has given **consent** to the processing of his or her personal data for one or more specific purposes;
b) processing is necessary for the **performance of a contract** to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract;
c) processing is necessary for compliance with a **legal obligation** to which the Data Controller is subject;
d) processing is necessary in order to protect the **vital interests** of the Data Subject or of another natural person;
e) 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 Data Controller; or

f) processing is necessary for the purposes of the **legitimate interests**[2] pursued by the Data Controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject which require protection of personal data, in particular where the data subject is a **child**.

Fairly – in order for processing to be fair, CEU must share certain information with the Data Subjects (private individuals) about the planned or ongoing data processing activity which shall be done in the form of a Privacy Notice.

Transparently – CEU has to give privacy-related information to Data Subjects which are detailed and specific, placing an emphasis on making Privacy Notices understandable and accessible. Information must be communicated to the Data Subject in an easily understandable form using clear and plain language and reflecting all details of the given data processing activity.

The specific information that must be provided to the Data Subject must, as a minimum, include:

- the identity and the contact details of the Data Controller and, if any, of the Data Controller's representative;
- the contact details of the DPO;
- the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
- whether the processing is based on the legitimate interests pursued by the Data Controller or by a third party;
- the period for which the personal data will be stored;
- the existence of the rights to request access, rectification, erasure, data portability, restriction of processing concerning the Data Subject or to object to the processing, and the conditions (or lack of) relating to exercising these rights, such as whether the lawfulness of previous processing will be affected;
- the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
- the categories of personal data concerned;
- the recipients or categories of recipients of the personal data, where applicable;
- that the Data Controller intends to transfer personal data to a third-party recipient and the level of protection afforded to the data;
- the right to lodge a complaint with the Authority;
- the existence of automated decision-making, including profiling at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the Data Subject;
- whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the Data Subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;
- the source of personal data if they have not been obtained from the Data Subject; and
- any further information necessary to guarantee fair and transparent processing.

2 Such legitimate interest could exist, for example, where there is a relevant and appropriate relationship between the Data Subject and the Data Controller in situations where the Data Subject is a client or in the service of the Data Controller. At any rate, the existence of a legitimate interest would need careful assessment including whether a Data Subject can reasonably expect at the time and in the context of the collection of the personal data that processing and for that purpose. The processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the Data Controller concerned. The processing of personal data for direct marketing purposes may also be regarded as carried out for a legitimate interest.

1.2 Personal data can only be collected for specific, explicit and legitimate purposes

It is the Data Owner's task to decide the specific and legitimate purpose and ground of the planned data processing activity and providing information about it through an adequate Privacy Notice. Personal data obtained for specified purposes must not be used for a purpose that differs from those formally defined in the Privacy Notice.

1.3 Personal data must be adequate, relevant and limited to what is necessary for processing ("Data minimization")

The Data Owners shall ensure that CEU does only collect personal data that is adequate, relevant and not excessive for the purpose for which it is obtained. In cases of doubt, the Data Owner shall consult the DPO. In any case, the Data Owner shall always observe the "Data minimization" principle.

All data collection forms (electronic or paper-based), must include a fair processing statement or link to Privacy Notice.

The Data Owners shall ensure that the collected personal data continues to be adequate, relevant and not excessive during the lifecycle of the personal data.

1.4 Personal data must be accurate and kept up to date

Data Owners shall be liable for reviewing and updating the personal data stored as necessary. No personal data should be kept unless it is reasonable to assume that it is accurate.

The Data Owner is responsible for ensuring that appropriate procedures and policies are in place to keep personal data accurate and up to date, taking into account the volume of data collected, the speed with which it might change and any other relevant factors.

On at least an annual basis, the Data Owner will review the retention dates of the personal data processed within his/her competence, and will identify any personal data that is no longer required in the context of the processing purpose.

The DPO is responsible for making appropriate arrangements that, where third-party organizations may have been passed inaccurate or out-of-date personal data, to inform them if it is possible and technically feasible that the information is inaccurate and/or out of date and is not to be used to inform decisions about the individuals concerned; and for passing any correction to the personal data to the third party where this is required.

1.5 Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing (storage limitation)

CEU shall not keep personal data in a form that permits identification of Data Subjects for a longer period than is necessary, in relation to the purpose(s) for which the personal data was originally collected.

During the processing period, personal data should be minimized/encrypted/pseudonymized if it is possible in order to protect the identity of the Data Subject in the event of a data breach.

Personal data will be retained in line with the corresponding Privacy Notice and, once its retention date is passed, it must be securely destroyed/deleted or anonymized.

The DPO must specifically advice any data retention that is planned to exceed the retention period defined in the corresponding Privacy Notice, and Data Owner must ensure that the justification is clearly identified and in line with the requirements of the data protection legislation.

CEU may store personal data for longer periods if the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes as well as in cases permitted by legitimate interest or required by law, subject to the implementation of appropriate technical and organizational measures to safeguard the rights and freedoms of the Data Subject.

Personal data must be disposed/deleted securely in an appropriate manner to maintain security and deletion process documented.

1.6 Personal data must be processed in a manner that ensures the appropriate security

All Members of CEU Community are responsible for ensuring that any personal data that CEU holds and for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorized by CEU to receive that information and has entered into a confidentiality agreement.

In determining the appropriate data security level, the Data Owner should consider the extent of possible damage or loss that might be caused to individuals (e.g. applicants, subscribers) if a security breach occurs, the effect of any security breach on CEU itself, and any likely reputational damage including the possible loss of customer trust.

When assessing appropriate technical measures, the Data Owner will consider the following:

- Password protection;
- Role-based access rights including those assigned to temporary staff: all personal data should be accessible only to those who need to use it, and access may only be granted in line with the rules established by the IT Department;
- The appropriate training levels throughout the unit/department running the data processing activity;
- The consultation of contractual obligations and taking appropriate security measures when transferring data to third parties, especially outside the EEA;
- All personal data should be treated with the highest security and must be kept
    - in a lockable room with controlled access; and/or
    - in a locked drawer or filing cabinet; and/or
    - stored on (removable) computer media which are password protected and encrypted.
- Care must be taken to ensure that PC screens and terminals are not visible except to authorized Members of CEU Community;

- Manual records (hard copies) may not be left where they can be accessed by unauthorized personnel and may only be removed from CEU's premises in case of necessity.

The evolving technical data security measures are elaborated and communicated by the IT Department on the IT intranet.

4. Privacy Notices

4.1 Whichever legal basis is being relied upon, Data Subjects need to be informed about how their personal data will be processed. This is done through statements that usually are known as Privacy Notices. These documents must provide information at the time of collecting the personal data, however, there might be different timeframes for cases out of the general rule. Personal data collected for the purpose(s) stated in the corresponding Privacy Notice can only legitimately be processed for those purpose(s) and not for others of which the Data Subject has not been informed (e.g. information collected on job application forms should be used for the recruitment process, and not to send the applicants general information about forthcoming CEU events).

4.2 Core Privacy Notices

CEU has a number of core Privacy Notices aimed at different, well identifiable types of data subjects: pre-applicants (whether undergraduate or graduate), applicants, students, alumni, supporters, job applicants, employees and website visitors. These Privacy Notices are supplied to these individuals at the relevant time as part of centrally managed processes (e.g. application or registration).

4.3 Supplementary or individual Privacy Notices

These core Privacy Notices can be supplemented as necessary by individual Privacy Notices of Departments, Units who wish to initiate a data processing within their competence related to any particular event, newsletter, video recording, initiative, service, grant provision, educational program or function that they might run.

4.4 The Data Owner is responsible for ensuring that the Privacy Notice(s) within his/her competence is correct, factually accurate and prepared in accordance with the legal requirements and that mechanisms exist for the proper communication of the Privacy Notice(s) on CEU's website(s) or otherwise to make all Data Subjects aware of the contents of this notice prior CEU commencing collection of their personal data. Privacy Notice is a public document that should be easily accessible for the Data Subject any time during the processing activity. All information provided to the Data Subject, including the Privacy Notice itself is in an easily accessible format (PDF, printed letter, or email), concise, transparent, intelligible using clear and plain language.

4.5 The Privacy Notice preparation procedure should include:
a) the identification of the purpose and the legal ground,
b) preparation of a DPIA if it is requested,
c) elaboration of the "balancing test" (or Legitimate Interest Assessment (LIA)) is the data processing is based on CEU's or third party's legitimate interest,
d) existence of GDPR Art. 9. legal ground is ensured in case special category of personal data is to be processed,
e) the collection and documentation of consent is ensured in case processing is based on consent,

f) when personal data is contractually required for processing, the underlying contract must be published to and accepted by the individual, and
g) the processing activity be registered in the Record of Processing Activities (ROPA).

5. Third Party Data Processors

5.1 Where processing is to be carried out on behalf of CEU by a third party entity (external companies, service providers), responsibility for the compliant, safe and appropriate use of the personal data at the processor remains with CEU. CEU shall only use processors providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of applicable laws and ensure the protection of the rights of the Data Subject. Reasonable steps must be taken to check if the security measures are adequate and in place.

5.2 The legal relationship between CEU and the data processor shall be governed in detail by a contract made out in writing between CEU and the data processor or made out by way of electronic means, or by any other legal act within the Austrian Data Protection Act and binding legislation of the EU. This written contract (**data processing agreement**) must regulate what personal data will be processed and how, what the processing activities are, for what purpose the personal data must be used and for how long.

5.3 Data Owners are liable for using only those data processors that are contractual partners of CEU by a data processing agreement or similar document. Freely available cloud-based services shall not be used for storing and processing any personal data related to CEU. (e.g. gmail or other e-mail service providers, dropbox, doodle)

5.4 CEU shall be held liable for selecting the data processor and the lawfulness of the instructions given to the data processor.

For further guidance about the use of third-party data processors please contact the GDPR Team.

6. Data Subjects' Rights

6.1 Data Subjects have the following rights regarding personal data processing, and the personal data that is recorded about them:
- To **be informed** of the circumstances of data processing before the commencement of processing.
- To obtain from the Data Controller confirmation as to whether or not personal data concerning him or her are **being processed**.
- To request the Data Controller to **make available** his or her personal data and information concerning the processing thereof (right to access).
- To take action to **rectify, restrict**. The Data Subject is entitled to the right to rectify without any undue delay inaccurate information concerning them.
- To ask CEU to **erase** personal data without delay:
  a. if it is no longer necessary in relation to the purposes for which it was collected or otherwise processed;
  b. if the only legal basis of processing is Consent and that Consent has been withdrawn and there is no other legal basis on which we can process that personal data;
  c. if the Data Subject objects to our data processing where the legal basis is the pursuit of a legitimate interest or the public interest and we can show no overriding legitimate grounds or interest;

d. if the Data Subject has objected to our processing for direct marketing purposes;
e. if the processing is unlawful.

- To not be the subject to decisions based solely on **automated processing** which produces legal effects concerning him or her or similarly significantly affects him or her and to be informed about the mechanics of occurring automated decision-making processing.
- To have personal data provided to them in a structured, commonly used and machine-readable format, and the right to have that personal data transmitted to another data controller (**data portability**).
- To **object** to, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on the legitimate interest of Data Controller, including Profiling.
- To withdraw his/her consent at any time where the legal basis of the processing is consent.
- To prevent the use of the personal data for direct marketing purposes.
- To request the Authority to assess whether any provision of the GDPR has been contravened.
- To sue for compensation if the Data Subject suffers damage by any contravention of the GDPR.

7. Subject Access Request Procedure ("SAR")

7.1 CEU ensures that Data Subjects may exercise these rights:

- Data Subjects may make data access requests as they wish. CEU will ensure that its response to the data access request complies with the requirements of the GDPR.
- Data Subjects have the right to complain to CEU related to the processing of their personal data and/or how complaints have been handled.

7.2 The Data Subject provides CEU with evidence of his/her identity and or any identification data before handling over data to him/her.

7.3 The Data Subject can request all data held on him/her or specific set of data held by CEU.

7.4 CEU provides the requested information to the Data Subject within one month from this recorded date. This period may be extended by two further months where necessary, taking into account the complexity and number of the requests. CEU informs the Data Subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the Data Subject makes the request by electronic means, the information shall be provided by electronic means where possible, unless otherwise requested by the Data Subject.

7.5 Once received, the SAR application shall be immediately forwarded to the DPO who will ensure that the requested personal data is collected within the specified time frame.
Collection entails:

- Collecting the personal data specified by the Data Subject, or
- Searching all live databases and all relevant filing systems (manual files) at CEU.

7.6 If CEU decides not to comply with the request, the DPO must respond to the Data Subject and explain its reasoning and inform him/her of the right to complain to the Authority and seek judicial remedy.

7.7 CEU removes personal data from systems and processing operations as soon as a request for erasure has been submitted by the Data Subject and deletion is justified by CEU and no other legal grounds requires the further storage of the personal data.

7.8 CEU, if it is feasible, contacts and communicates with other organizations, where the personal data of the Data Subject is being processed due to transfer initiated by CEU, to cease processing information at the request of the Data Subject.

7.9 CEU makes all necessary measures without undue delay in the event that the Data Subject has withdrawn consent or objects to the processing of their personal data in whole or in part.

8. Consent

Whenever the personal data processing is based on consent, the following prerequisites must be met and documented by the Data Owner.

8.1 CEU understands 'consent' to mean that:
a) it has been explicitly and voluntarily given, and a specific, informed and unambiguous indication of the Data Subject's wishes that, by statement or by a clear affirmative action to the processing of personal data relating to him or her. The Data Subject can withdraw the consent at any time.
b) the Data Subject has been fully informed of the intended processing and consent obtained on the basis of misleading or unprecise information will not be a valid basis for processing.

8.2 CEU must demonstrate that the consent has been actively given (e.g. signed/ticked consent form, Privacy Notice accepted by the Data Subject before information is being processed, etc.). Consent cannot be implied (non-response to a consent request).

8.3 For special categories of data, explicit written consent of Data Subjects must be obtained unless an alternative legitimate basis for data processing exists in which case consultation with the GDPR Team is advised.

9. Non-disclosure of personal data

CEU must ensure that personal data is not disclosed to unauthorized third parties which includes family members, friends, government bodies, and in certain circumstances, the police or public. All Members of CEU Community should exercise caution when asked to disclose personal data held on another individual to a third party or to the public.

Appropriately anonymized statistical data based on personal data which was prepared by CEU may be disclosed.

All requests to provide personal data must be supported by appropriate documentation and handled by the DPO.

No personal data should be altered, concealed, blocked or destroyed once a request for access (SAR) has been made. The Data Owner should contact the GDPR Team before any changes are made to personal data which is the subject of an access request (SAR).

10. Data Transfers and data export

10.1 All exports of data from within the EEA[3] to non-European Economic Area countries (referred to in the GDPR as 'third countries') are unlawful unless there is an appropriate "level of protection for the fundamental rights of the data subjects".[4]
10.2 The transfer of personal data outside of the EEA is prohibited unless one or more of the specified safeguards, or exceptions, apply:

1. An adequacy decision

The European Commission can and does assess third countries, a territory and/or specific sectors within third countries to assess whether there is an appropriate level of protection for the rights and freedoms of natural persons. In these instances, no authorisation is required.
Countries that are members of the EEA but not of the EU are accepted as having met the conditions for an adequacy decision.[5]

2. Privacy Shield

In its judgment of July 16, 2020, C-311/18, the ECJ declared the adequacy decision regarding the USA ("EU - US Privacy Shield") to be invalid.

Chapter V (Transfer of personal data to third countries or to international organizations) of the GDPR also provides other means for lawful data transfer to third countries, above all Standard Contractual Clauses (SCC), the validity of which the ECJ confirmed in the judgment cited above, as well as binding internal data protection regulations (Binding Corporate Rules - BCR); see more information about SCCs and BCRs below. However, it is only possible to invoke these data transfer mechanisms, if additional security guarantees are included. The data exporter in the EU, in cooperation with the data importer in the third-country, is responsible for such additional security guarantees.

3. Binding corporate rules

CEU may adopt approved binding corporate rules (BCR) for the transfer of personal data outside the EU which are essentially data protection policies governing transfers made between organisations within a group for transfers of personal data outside of the EU. This requires submission to the Authority for approval of the rules that CEU is seeking to rely upon.

4. Standard contractual clauses (SCC)

CEU may adopt approved model contract clauses for the transfer of data outside of the EEA. If CEU adopts the standard data protection clauses adopted by the Commission, there is an automatic recognition of adequacy.

For further guidance about the transfer of personal data within or outside the EU, please contact the GDPR Team.

[3] EEA: Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and UK, and also Iceland, Liechtenstein and Norway.
[4] The broader area of the EEA is granted 'adequacy' on the basis that all such countries are signatories to the GDPR. The non-EU EEA member countries (Liechtenstein, Norway and Iceland) apply EU regulations through a Joint Committee Decision.
[5] A list of countries that currently satisfy the adequacy requirements of the Commission are published in the *Official Journal of the European Union.* http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm

11. Record of Processing Activities (ROPA) /Data map

CEU shall maintain a record of all processing activities (ROPA) under its responsibility.

11.1 CEU's ROPA consists of the individual ROPAs or data maps prepared and kept up-to-date by the Data Owners concerning the processing activities within their competence.

11.2 The data map determines - among others - the following:

- indication of processes that use personal data and the unit/department responsible for it;
- source and type of personal data;
- volume of data subjects;
- processing activity;
- the legal basis and the purpose(s) for which personal data is used;
- internal and external recipients of the personal data;
- key systems and repositories, location of the data;
- any data transfers; and
- all retention and disposal requirements.

The GDPR Team will provide the template ROPA documents to be filled in by the Data Owners on their request.

12. Data Privacy by Design and Privacy by Default and Data Protection Impact Assessments (DPIAs)

The concept of 'data protection by design' means embedding data protection considerations at an early stage of any new process, project or procedure. CEU should implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. (**Privacy by Design)**

12.1 There are seven principles in the concept of Privacy by Design and each of them have equal importance. These principles are:

1. Proactive not Reactive/Preventative not Remedial: data privacy needs to come up at the beginning of the planning process;
2. Privacy as the Default: privacy needs to be at the forefront of what we plan to do or actually do;
3. Privacy Embedded into Design: privacy is a core feature of the activity where encryption, authentication should be used and testing vulnerabilities on a regular basis.
4. Full Functionality: a balance between growth and security, functionality and privacy;
5. End-to-End Security: privacy protection follows data through the lifecycle from collection to deletion/archival;
6. Visibility and Transparency: privacy isn't just for privacy's sake; Data Subjects should know about CEU's privacy (and processing) practices and CEU should be open about it;
7. Respect for User Privacy: data processing needs to remain user-centric because even if CEU has the data, it nevertheless belongs to the individual CEU collected it from.

12.2 In addition to the above, CEU need to ensure that, by default, only personal data which is necessary for each specific purpose of the processing is processed (**Privacy by Default**). The obligation applies to the volume of personal data collected, the extent of the

processing, the storage period and the accessibility of the personal data. In particular, by default, personal data should not be available to an indefinite number of persons.

12.3 Where a type of processing, in particular 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, CEU shall, prior to the processing, carry out a DPIA of the impact of the envisaged processing operations on the protection of personal data. A single DPIA may address a set of similar processing operations that present similar high risks.

12.4 The Data Owner should conduct a DPIA and record the findings in the following circumstances:
1. the use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);
2. automated processing including Profiling;
3. large scale processing of sensitive (special category) data; and
4. large scale, systematic monitoring of a publicly accessible area.

12.5 There might be other occasions when under the data protection by design approach the need for a DPIA might arise to assess and document the risks to Data Subjects and the mitigation measures that might be implemented. Austrian legislation must always be checked for cases (see Annex 1) when mandatory requirement is the preparation of the DPIA ("black list").

12.6 A DPIA must include:
- a description of the processing, its purposes and the Data Controller's legitimate interests if appropriate;
- an assessment of the necessity and proportionality of the processing in relation to its purpose;
- an assessment of the risk to individuals; and
- the risk-mitigation measures in place and demonstration of compliance.

When identifying privacy risks the following steps must be followed:

1) Identifying and describing the privacy risk associated to that processing activity;
2) Using the likelihood criteria (1 – low, 2 – medium and 3 - high), scoring the likelihood of the risk occurring;
3) Using the impact criteria (0 – zero impact, 1 – low, 2 – medium and 3 - high) of the risk should it occur;
4) Producing a calculated risk, identifying the risk to the rights and freedoms of data subjects and assessing the risks to the business (including reputational damage); and
5) Identifying solutions to privacy risks, assigning risk treatment measures.

12.7 Where, as a result of a DPIA, it is clear that CEU is about to commence processing of personal data that could cause damage and/or distress to the Data Subjects, the decision as to whether or not CEU may proceed must be escalated for review to the DPO. The DPO shall, if there are significant concerns, either as to the potential damage or distress, or the quantity of personal data concerned, escalate the matter to the Authority.

13. Direct Marketing

13.1 Direct marketing is defined as the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals. This is a broad definition that is not restricted to commercial organisations offering goods for sale. The term direct marketing also applies to communications addressed to individuals that promote an organisation's aims and ideals, including advertising events, offering benefits or appealing for funds and support.

13.2 CEU is subject to the Austrian Telecommunications Act and privacy laws when marketing to applicants, students, alumni and any other potential users of its services. In case of breach of the provisions of the Austrian Telecommunications Act, managerial liability might be applicable meaning that not only CEU faces potential fines or other legal consequences, but its first manager or the managing body.

13.3 Direct marketing by email (or text) should normally only take place with the individual recipient's prior consent (i.e. they have opted in to receive the emails or texts).

13.4 There should be a clear unsubscribe opportunity in each email, text or phone communication which is an absolute right and opt-outs must be fully respected.

13.5 Many marketing communications are sent to alumni, applicant, supporters, etc. in newsletters as various mailing lists maintained both centrally and by units/departments exist to advertise events, activities or initiatives to members of the public (including, for example, attendees at public events or academics at other universities).

14. Processing special category (sensitive) personal data

Certain types of personal data are defined in the GDPR and applicable data protection legislation as more sensitive than others. These are known as special category personal data and relate to personal data about:

- Racial or ethnic origin.
- Political opinions.
- Religious or philosophical beliefs.
- Trade Union membership.
- Genetic data.
- Biometric data.
- Health data.
- Sex life or sexual orientation.

The processing of special category personal data requires legal basis under art. 6 and 9. of the GDPR. For identifying the appropriate legal basis, the Data Owner should consult the GDPR Team.

Performance of non-discrimination and its monitoring, academic research and the provision of welfare and support services or specific grants to staff, students or third parties, are many of the occasions when special category personal data might need to be processed by CEU.

15. Personal Data Breach Notification Procedure

When the security of personal data is breached, the personal data might get lost, stolen, inadvertently disclosed to an external party, accidentally published or unauthorized access to the data may occur.

15.1 Examples of information security incidents include but are not limited to;

- Unauthorised or accidental disclosure of personal data; e.g. email sent to incorrect recipients; personal data of students mistakenly sent to the wrong mailing list; an e-mail is sent to recipients in the "to:" or "cc:" fields, thereby enabling each recipient to see the email address of other recipients.

- Unauthorised modification of personal data; e.g. altering master copy of student or staff record.

- Unauthorised access to CEU's information systems/mobile device/e-mail account; e.g. example virus, malware,; as a result of a cyber attack on that of an online service, personal data of individuals are exfiltrated; CEU suffers a ransomware attack which results in personal data being encrypted; an online service provider third party company acting as a data processor identifies an error in the code concerning authorisation which means that any user can access the account details of any other user.

- Unauthorised access to areas containing IT equipment which stores personal data; e.g. unauthorised entry into a data center or network cabinet rooms.

- Theft or Loss of personal data; e.g. hard copy stolen from bag or left in café.

- Theft or loss of equipment that contains personal data; e.g. laptop/mobile phone/USB drive stolen from bag or left at conference.

15.2 All users (whether Members of the CEU Community, contractors or temporary employees and third party users) of CEU are required to be aware of, and to follow this procedure in the event of a personal data breach and report the breach as soon as possible to the DPO.

15.3 Breach notification: data controller to Authority

The DPO documents the information received on the potential breach and in cooperation with the Data Owner (Breach Investigation Team (BIT)) (i) contacts any Member of the CEU Community who might have relevant information and/or data processor(s) involved in the breach and (ii) assesses the circumstances of the incident:

- In some cases, it is obvious that personal data breach has occurred (e.g. an email has been sent to the wrong recipient, hackers gain access to the data, ransomware attack, etc.) and the DPO will advise on straightforward remedial actions, if these have not been taken already (e.g. asking the incorrect recipient of the email to delete it, separate the affected database, etc.).

- In other cases, more detailed/technical investigations may be required to ascertain the facts of what has happened, involving colleagues who understand the information in scope and/or the checking of logs by IT specialist, and to determine what remedial

technical or organisational actions are required and which colleagues need to be informed and act. This assessment is necessary to ascertain whether or not there is any evidence that a personal data breach has actually occurred (as opposed to a "simple" security incident).

The BIT assesses whether the personal data breach is likely to result in a risk to the rights and freedoms of the Data Subjects affected by the personal data breach, by evaluating the real and potential consequences of the breach to the affected individuals.
The DPO and the management of CEU determines if the Authority need to be notified in the event of a breach.

If a risk to Data Subject's rights and freedom is likely, CEU reports the personal data breach to the Authority without undue delay, and not later than 72 hours.

If the data breach notification to the Authority is not made within 72 hours, CEU's DPO is required to submit it electronically with a justification for the delay.

If it is not possible to provide all of the necessary information at the same time, CEU will provide the information in phases without undue further delay.

15.4 Breach notification: data controller to data subject

The BIT will determine whether there is a *high risk* to the Data Subjects' rights and freedom and that they need to be informed about the personal data breach directly. If the personal data breach is likely to result in high risk to the rights and freedoms of the Data Subject, CEU notifies those/the Data Subjects affected immediately in accordance with the BIT's and Communications Office's recommendations.

The notification to the Data Subject describes the breach in clear and plain language, subsequent steps have been taken to ensure that the risk is unlikely to materialise, security measures were applied to render the personal data unintelligible (e.g. encryption) or it would amount to disproportionate effort to inform the Data Subject directly.

If the breach affects a high volume of Data Subjects and personal data records, CEU makes a decision based on assessment of the amount of effort involved in notifying each Data Subject individually, and whether it will hinder CEU's ability to appropriately provide the notification within the specified time frame. In such a scenario a public communication or similar measure shall be made to inform those affected in an equally effective manner.

The DPO documents any personal data breach(es) into the Breach Registry, incorporating the facts relating to the personal data breach, its effects and the remedial action(s) taken.

16. Training

The management of CEU promotes training and awareness programmes for the Members of the CEU community, and CEU shall make resources available in order to raise awareness.

The DPO shall demonstrate and communicate to Members of the CEU Community the importance of data protection in their role and ensure that they understand how and why personal data is processed in accordance with CEU's policies and procedures through online or offline trainings.

DPO ensures that Members of the CEU Community are kept up to date and informed of key issues and legal developments related to the treatments of personal data.

The DPO is responsible for organising specific training occasions for Data Owners or colleagues in charge of dealing with personal data in case it is needed.

17. Data protection in the course of scientific research

In the course of managing data for scientific research, CEU ensures that the rights of the data subject to the protection of his/her personal data are provided in line with the applicable Austrian and EU data protection rules, as laid down in this Policy. Specific and more detailed provisions are indicated in CEU's Ethical Research Policy.

Members of the CEU Community initiating research must ensure that privacy issues are adequately handled, DPIA is prepared if it is needed and research participants are informed on the processing of their personal data throughout the research activity by individual Privacy Notices or otherwise before they become a member of the research group.

18. Data Security

The Data Owner is responsible for ensuring personal data security, the level of which depends upon the nature of individual personal data and the planned processing activity.

Any personal data can be represented both electronically (personal data that are created or stored on electronic media) and non-electronically (e.g., personal data created or stored on paper, including hard copies of electronically stored documents).

Electronically stored data

Most of the electronically stored personal data security measures are determined and implemented by the IT Department. However, the Data Owner is responsible for the proper use of those measures and/or additional safeguards.

Security measures at CEU might include:

- Regularly patched and updated operating systems
- Anti-virus and anti-malware software on the operating systems
- Firewall-protected on-premises network and automated intrusion detection/prevention systems
- Disk-level encryption of hard drives to protect files and folders stored there
- Strong preference for using only such online services where data is encrypted both at-rest and in-transit
- The location of personal data within the EU whenever is possible
- Limiting the use of such 3rd party online services for storing data, where CEU and the 3rd party service provider (as data processors) does not have a data protection agreement signed. (e.g., members of CEU Community's private e-mail addresses or private file storage solutions must not be used for collecting, storing personal data during data processing activity performed by CEU. Please, also see provisions in section 5.3.)

Non-electronically stored data

Most of the non-electronically stored data security measures are determined and implemented by the Office of the Director of Facilities. However, the Data Owner is responsible for the proper use of those measures and/or additional safeguards.

Security measures at CEU might include:

- Physical security controls - such as card-accessed buildings, locked rooms, locked filing cabinets.
- safeguards to ensure CEU's ability to restore the availability and access to personal data in a timely manner in the event of a physical incident.

General Principles

1. CEU controls access to information based on business and security requirements.
2. Access control rules and rights to applications, expressed in standard user profiles, for each user / group of users are clearly stated, together with the business requirements met by the controls.
3. The security requirements of each business application are determined by a risk assessment that identifies all information related to the application and the risks to that information.
4. The access rights to each application take into account:
    a. Premises access control – unauthorized persons are prevented from gaining physical access to premises, buildings or rooms where data processing systems are located.
    b. System access control – access to data processing systems is prevented from being used without authorization.
    c. Data access control – Persons entitled to use a data processing system gain access only to the data to which they have a right of access.
    d. Personal data cannot be read, copied, modified or removed without authorization.
    e. The 'need to know' principle (i.e., access is granted at the minimum level necessary for the role).
    f. Everything is generally forbidden unless explicitly permitted.
    g. Any privileges that users need to perform their roles, subject to it being on a need-to-use and event-by-event basis.
5. CEU has standard user groups for common roles in CEU.
6. User access requests, authorization and administration are segregated as described.
7. User access requests are subject to formal authorization, to periodic review and to removal.

19 Closing Provisions

19.1 Matters that are not covered by this Policy shall be governed by the relevant laws and other data protection rules, as applicable.

19.2 The present Policy will come into force upon approval by the Senior Leadership Team which date should be reflected on the cover page of this Policy.

Annex 1

Key elements of Austrian law incorporating data privacy requirements are the following at the time of the approval of the present Policy:

1. Austrian Data Protection Act (Datenschutzgesetz, BGBl I 1999/165 idgF; "**DSG**"),

2. the Austrian Private University Act (Privathochschulgesetzgesetz, BGBl I BGBl. I Nr. 77/2020 idgF; "**PrivHG**;),

3. the Austrian Education Documentation Act (Bildungsdokumentationsgesetz, BGBl I 2002/12 idgF; "**BilDokG**")

4.the Austrian Higher Education Quality Assurance Act (Hochschul-Qualitätssicherungsgesetz, BGBl I 2011/74 idgF; "**HS-QSG**")

5. the Austrian Research Organization Act (Forschungsorganisationsgesetz, BGBl 1981/341 idgF; "**FOG**"),

6. the Austrian Telecommunications Act (Telekommunikationsgesetz 2003 - TKG 2003)

7. DPIA black list/white list laws:

- Datenschutz-Folgenabschätzung ,

- Verordnung der Datenschutzbehörde über Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung durchzuführen ist (DSFA-V) StF: BGBl. II Nr. 278/2018

- Verordnung der Datenschutzbehörde über die Ausnahmen von der Datenschutz-Folgenabschätzung (DSFA-AV) StF: BGBl. II Nr. 108/2018

Annex 2
Definitions, explanation of personal data

The term '**personal data'** is the key notion to the application of the GDPR. Only if processing of data concerns personal data, the GDPR applies. The term is defined in Art. 4 (1) of the GDPR: personal data are any information which are related to an identified or identifiable natural person.

The data subjects are identifiable if they can be directly or indirectly identified, especially by reference to an identifier such as a name, an identification number, location data, an online identifier or one of several special characteristics, which expresses the physical, physiological, genetic, mental, commercial, cultural or social identity of these natural persons. In practice, these also include all data which are or can be assigned to a person in any kind of way. For example, the telephone, credit card or personnel number of a person, account data, number plate, appearance, customer number or address are all personal data.

Since the definition includes "any information," it must be assumed that the term "personal data" should be as broadly interpreted as possible. This is indicated in the case law of the European Court of Justice, which also considers less explicit information, such as recordings of work times which include information about the time when an employee begins and ends his workday, as well as breaks or times which do not fall in work time, as personal data. Also, written answers from a candidate during a test and any remarks from the examiner regarding these answers are "personal data" if the candidate can be theoretically identified. The same also applies to IP addresses. If the controller has the legal option to oblige the provider to hand over additional information which enable him to identify the user behind the IP address, this is also personal data.

In addition, personal data need not be objective. Subjective information such as opinions, judgements or estimates can also be personal data. This includes an assessment of creditworthiness of a person or an estimate of work performance by an employer.

An individual is 'identified' or 'identifiable' if you can distinguish them from other individuals. A name is perhaps the most common means of identifying someone. However, whether any potential identifier actually identifies an individual depends on the context. A combination of identifiers may be needed to identify an individual. The GDPR provides a non-exhaustive list of identifiers, including: name; identification number; location data; and an online identifier (IP addresses and cookie identifiers).

In addition to general personal data, one must consider above all the special categories of personal data (also known as sensitive personal data) which are highly relevant because they are subject to a higher level of protection. These data include genetic, biometric and health data, as well as personal data revealing racial and ethnic origin, political opinions, religious or ideological convictions or trade union membership.

Anonymous data: Data which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or is no longer identifiable.

Authority: Austrian National Authority for Data Protection (Österreichische Datenschutzbehörde) is the designated supervisory authority being responsible for monitoring the application of GDPR, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the European Union.

Biometric data: Personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopy data.

Breach Registry: A Data Breach Register is a register to record all data breaches within CEU's privacy network.

Consent: In cases where CEU is obliged to collect or transfer personal data based on a legal requirement (including the request of national authorities), it will not require the consent of the data subject for processing his/her personal data. If there is no other legal basis for the data processing, CEU shall request the freely given and explicit consent of all data subjects for the processing of their personal data before actual data processing takes place.

Consent of the data subject: Any freely, voluntary given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Data collected: CEU collects and uses personal data about its students, faculty and staff, as well as other individuals who come into contact with CEU. This data is gathered in order to enable CEU to provide education and other associated functions and activities in line with the applicable legal provisions.

Data concerning health: Personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

Data Controller: The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by European Union or Member State law, the controller or the specific criteria for its nomination may be provided for by European Union or Member State law.

Data Owner: Head of Unit or Department within CEU that decides, manages the data processing activities within his or her competence and is liable and accountable for the protection of personal data. Each Data Owner shall designate a Data Steward.

Data Processing: Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use,

disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Data Processor: Means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Data Controller.

Data Protection Officer: Means the person appointed by CEU who must inform and advise on the protection of personal data in relation to the GDPR, national law(s) and regulations and the Policy (hereinafter: "DPO").

Data Steward: Means the designated liaison(s) by a Data Owner, who manages the data ownership tasks with the DPO.

Data Subject: Any living individual who is the subject of personal data held by an organization.

Legal Requirements: In specific cases, there may be a legal requirement to collect, use and/or transfer specific personal data to ensure that CEU complies with its statutory obligations related to its operation as a higher education institution in Austria. CEU may also be requested by the national authorities in the course of its proceedings to provide specific personal data managed by it about its students, faculty and staff, as well as individuals who come into contact with CEU during its operation.

Legitimate Interest Assessment (LIA): or the "balancing test" is a three part test which requires you to identify your legitimate interest, show that the processing activity is necessary to achieve that legitimate interest and balance the processing activity against the rights and freedoms of the Data Subject.

Members of the CEU Community: Includes students, management, faculty and staff of CEU as well as other individuals providing educational services to or conducting research at CEU.

Personal data breach: A breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed. There is an obligation on the Data Controller to report personal data breaches to the Authority and where the breach is likely to adversely affect the personal data or privacy of the Data Subject.

Privacy Notice: A statement made to a Data Subject that describes how CEU collects, uses, retains and discloses personal information. Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the GDPR.

Profiling: Any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyze or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behavior. This definition is linked to the right of the Data Subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.

Pseudonymisation: The processing of personal data in such a manner that the personal data can no longer be attributed to a specific Data Subject without the use of additional information, provided that such additional information is kept separately and is subject to

technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Public Disclosure: Making personal data available to the general public.

Special categories of personal data or sensitive data: Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Third party: A natural or legal person, public authority, agency or body other than the Data Subject, Data Controller, Data Processor and persons who, under the direct authority of the Data Controller or Data Processor, are authorized to process personal data.

Data transfer to third country(ies)/data export/international data transfer: When personal data are transferred to a third country (a country outside the EEA), for example when personal data are stored on servers located in a third country. Remote access from a third country (for example in support situations) and/or storage in a cloud situated outside the EEA, is also considered to be an international data transfer. Data transfer might occur with the involvement of various service providers, for example when the Data Processor outside the EEA transfers the personal data to a sub-processor in another third country or in the same third country.

Signed by *CEU President and Rector Shalini Randeria.*
The original document is filed at the Office of the Academic Secretary.

Document information	
Type	Policy
Number	P-2112
Title	Data Protection Policy
Distribution	Internal
Filename	P-2112 CEU PU Data Protection Policy
Notes	
Related documents	
For final documents	
Approved by:	Senate
Date of approval	December 10, 2021
Enters force	December 10, 2021