Data Protection Policy of **Közép-európai Egyetem,** **Central European University** **and** **CEU Educational-Service Non-profit Llc.**	**A Közép-európai Egyetem,** **a Central European University** **és** **a CEU Oktatási-Szolgáltató Nonprofit Kft.** **Adatvédelmi Szabályzata**

2019
Budapest

Contents

Overview of the Data Protection Policy

This Data Protection Policy (hereinafter the: "Policy") was prepared and issued by Közép-európai Egyetem (hereinafter: "KEE"), Central European University, New York (hereinafter: "CEU NY") and CEU Educational-Service Non-profit Llc. (hereinafter:"CEU Llc.") (KEE, CEU NY and CEU Llc. hereinafter jointly as: "CEU") as joint data controllers (hereinafter: "Joint Data Controllers") in order to comply with the applicable data privacy requirements, including specifically the EU General Data Protection Regulation (hereinafter: "GDPR")[1], Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information (hereinafter: "Hungarian Data Protection Act") and Act CCIV of 2011 on National Higher Education (hereinafter: "NHEA").

The following overview provides a brief introduction to how personal data is handled by CEU.

Joint Data Controllers: KEE, CEU NY and CEU Llc. jointly determine the purposes and means of data processing, therefore, they qualify as joint controllers under Article 26 of the GDPR. The respective responsibilities of Joint Data Controllers for compliance with the obligations under the applicable rules are determined in a Joint Data Controllers' Agreement concluded between KEE, CEU NY and CEU Llc. (please see point 4.).

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.

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 Hungary. 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, staff, as well as individuals who come into contact with CEU during its operation.

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.

Data Protection Policy: the detailed rules on how CEU handles personal data can be found in the present Policy, taking into consideration also the Joint Data Controllers' Agreement concluded between KEE, CEU NY and CEU Llc. (please see point 4.). The Policy is intended to ensure that personal data is dealt with correctly and securely and in accordance with the applicable national laws and the laws of the European Union (hereinafter: "EU"). It applies to all personal data managed by CEU regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically. All members of CEU involved in the collection, processing and disclosure of personal data shall be aware of their duties and responsibilities related to personal data management by fully adhering to this Policy.

[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.

1. **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 Hungarian and EU data protection rules, as laid down in this Policy. Specific and more detailed provisions are indicated in CEU's Ethical Research Policy.

Background

The GDPR replaces the EU Data Protection Directive of 1995[2] ("Directive") and supersedes the laws of individual EU Member States that were developed in compliance with the Directive. Its purpose is to protect the "rights and freedoms" of natural persons (i.e. living individuals) and to ensure that personal data is not processed without their knowledge, and, wherever possible, that it is processed with their consent.

The Hungarian Data Protection Act provides further, more specific provisions for the national implementation of the GDPR.

2. Scope

2.1 Material scope of the GDPR

The GDPR applies to the processing of personal data wholly or partly by automated means (i.e. by computer) and to the processing other than by automated means of personal data (i.e. paper records) that form part of a filing system or are intended to form part of a filing system.

2.2 Territorial scope of the GDPR

The GDPR will apply to all controllers that are established in the EU or in the area of European Economic Area (hereinafter: EEA) who process the personal data of data subjects, in the context of that establishment. It will also apply to controllers outside of the EU that process personal data in order to offer goods and services, or monitor the behavior of data subjects who are resident in the EU.

2.3 Scope of the present Policy

Please see "Overview of the Data Protection Policy" above.

3. Definitions

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 no longer identifiable.

Authority - National Authority for Data Protection and Freedom of Information (Nemzeti Adatvédelmi és Információszabadság Hatóság - NAIH) 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 - means 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 dactyloscopic data.

Child – the GDPR defines a child as anyone under the age of 16 years old, although this may be lowered to 13 by Member State law. The processing of personal data of a child is only lawful

[2] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

if parental or custodian consent has been obtained. The controller shall make reasonable efforts to verify in such cases that consent is given or authorized by the holder of parental responsibility over the child.

Consent - of the data subject means 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.

Cross-border processing - means either:
(a) processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or
(b) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

Data concerning health - means 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 Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Data Owner – Unit or Department within CEU that manages and is accountable for the protection of personal data. Each Data Owner shall designate a Data Steward (please see Annex 37 – Organizational Structure).

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 (please see Annex 37 – Organizational Structure).

Data subject – any living individual who is the subject of personal data held by an organization.

Data subject consent **-** means any freely 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.

Establishment **–** the main establishment of the controller in the EU will be the place in which the controller makes the main decisions as to the purpose and means of its data processing activities. The main establishment of a processor in the EU will be its administrative center. If a controller is based outside the EU, it will have to appoint a representative in the jurisdiction in which the controller operates to act on behalf of the controller and deal with supervisory authorities.

Filing system – any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis.

Genetic data - means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.

Members of CEU Community – includes students, faculty and staff of CEU as well as other individuals providing educational services to or conducting research at CEU.

Personal data – any information relating to an identified or identifiable natural person ('data subject'); 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.

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 controller to report personal data breaches to the supervisory authority and where the breach is likely to adversely affect the personal data or privacy of the data subject.

Privacy Notice – 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 (please also see point 6.1 below and Annex 9 - Privacy Notice).

Profiling **–** is 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 - means 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 - means 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, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data.

4. Identity, contact details and representative of the Joint Data Controllers

4.1 Pursuant to Article 4 (7) of the GDPR, the following legal entities are considered to be data controllers who determine the purposes and means of processing personal data individually or with others:

Name:	**Közép-európai Egyetem**	**Central European University**	**CEU Educational-Service Non-profit Limited Liability Company**
Seat:	1051 Budapest Nádor u. 9.	224 West 57th street, New York, NY 10019, USA	1051 Budapest Nádor u. 9
Registration number	FI27861	24306	01-09-913820
Representative:	Michael Ignatieff, Rector	Michael Ignatieff, president and rector	Mark Kiss managing director
Phone:	+ 36 1 3273000	+ 36 1 3273000	+ 36 1 3273000

4.2 Pursuant to Article 26 of the GDPR, Joint Data Controllers determine, in a transparent manner their respective responsibilities for compliance with the obligations under GDPR and any other applicable data privacy requirements, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information by means of an arrangement (hereinafter: "Joint Data Controller Agreement") among them. The essence of the Joint Controller Agreement is available to the data subject at the all-time website of Joint Data Controllers.

4.3 For the purposes of having mutually-agreed and compliant access to any personal data held by the Joint Data Controllers, the KEE will act as the Lead Data Controller, coordinating the joint data management activities of the Joint Data Controllers and hosting the personal data collected through the course of this collaboration.

5. Policy Statement

5.1 The management of CEU is committed to comply with all relevant EU and national laws, as applicable, in respect of personal data, and the protection of the "rights and freedoms" of individuals whose information CEU collects and processes in accordance with the GDPR.

5.2 Compliance with the GDPR is described by this Policy and other relevant policies of CEU such as the Information Security Policy (Annex 1), along with connected processes and procedures.
5.3 This Policy applies to all of CEU's personal data processing functions, including those performed on customers', clients', employees', students, contractors', suppliers' and partners' personal data, and any other personal data the organization processes from any source.
5.4 CEU has established objectives for data protection and privacy, which are in the GDPR Objectives Record (Annex 2 – GDPR Objectives Record).
5.5 This Policy applies to all Members of CEU Community. Any breach of this Policy shall constitute a misconduct under CEU's Code of Ethics and may also be a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities.
5.6 Partners and any third parties working with or for CEU, and who have or may have access to personal data, will be expected to have read, understood and to comply with this Policy. No third party may access personal data held by CEU without having first entered into a data confidentiality agreement and a contract in accordance with Article 28 of GDPR, which imposes on the third party obligations no less onerous than those to which CEU is committed.

6. Responsibilities and roles under the GDPR

6.1. Joint Data Controllers (CEU) are data controllers and/or data processors under the GDPR.
6.2. The Administrative Management and all those in managerial or supervisory roles at CEU are responsible for developing and encouraging good information handling practices and data protection awareness within CEU. All Units, Departments and Centers as Data Owners shall designate a Data Steward who shall act as a liaison managing the data ownership tasks with the Data Protection Officer (please see Annex 37 – Organizational Structure)
6.3. Joint Data Controllers have appointed a common, joint Data Protection Officer (DPO).
6.4. The DPO is a role specified in the GDPR, the Hungarian Data Protection Act and in this Policy, in line with his/her Job Description (Annex 4 – DPO Job Description) and Data Protection Job Description Responsibilities (Annex 5 – DPO Responsibilities). The DPO shall be a member of the senior management team (see Annex 37 – Organizational Structure) accountable for the management of personal data within CEU and for ensuring that compliance with data protection legislation and good practice can be demonstrated. This accountability includes:
    (i) development and implementation of the GDPR and the related data protection laws as required by this policy; and
    (ii) security and risk management in relation to compliance with the Policy.
6.5. The DPO has been appointed to take responsibility for CEU' compliance with this Policy on a day-to-day basis and, in particular, has direct responsibility for ensuring that CEU complies with the GDPR.
6.6. The DPO has specific responsibilities in respect of procedures such as the Subject Access Request Procedure (Annex 6 – Subject Access Request Procedure) and is the first point of call for Members of CEU Community seeking clarification on any aspect of data protection compliance.
6.7. Compliance with data protection rules (including the applicable laws and this Policy) is the responsibility of all Members of CEU Community who process personal data.
6.8. CEU's Training Policy (Annex 7 - Training Policy) sets out specific training and awareness requirements in relation to specific roles and Faculty and Staff of CEU in general.
6.9. Members of the CEU Community are responsible for ensuring that any personal data about them and supplied by them to CEU is accurate and up-to-date.

7. Data Protection Principles

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

7.1. Personal data must be processed lawfully, fairly and transparently.

Lawful – identify a lawful basis 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 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 controller;
f) processing is necessary for the purposes of the **legitimate interests**[3] pursued by the 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.

These are often referred to as the "conditions for processing".

Fairly – in order for processing to be fair, the data controller has to make certain information available to the data subjects as practicable (Privacy Notice) (please see Annex 9 – Privacy Notice). This applies whether the personal data was obtained directly from the data subjects or from other sources.

Transparently – the data controller has to give privacy information (see Annex 9- Privacy Notice) 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 intelligible form using clear and plain language.

CEU's Privacy Notice Procedure is set out in Annex 8 – Privacy Procedure and provides further guidance on lawful, fair and transparent data processing. The Privacy Notice is recorded in Annex 9 – Privacy Notice.

3 Such legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the 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 for that purpose may take place. 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 be regarded as carried out for a legitimate interest.

The specific information that must be provided to the data subject must, as a minimum, include:

7.1.1 the identity and the contact details of the controller and, if any, of the controller's representative;
7.1.2 the contact details of the DPO;
7.1.3 the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
7.1.4 where the processing is based on the legitimate interests pursued by the controller or by a third party (see – 7.1. f))
7.1.5 the period for which the personal data will be stored;
7.1.6 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;
7.1.7 the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
7.1.8 the categories of personal data concerned;
7.1.9 the recipients or categories of recipients of the personal data, where applicable;
7.1.10 where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organization and the level of protection afforded to the data;
7.1.11 the right to lodge a complaint with a supervisory authority;
7.1.12 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.
7.1.13 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
7.1.14 the source of personal data if they have not been obtained from the data subject
7.1.15 any further information necessary to guarantee fair and transparent processing.

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

Personal data obtained for specified purposes must not be used for a purpose that differs from those formally defined in the Privacy Notice. Privacy Notice Procedure (Annex 8) sets out the relevant procedures.

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

7.3.1 The DPO is responsible for ensuring CEU does not collect personal data that is not strictly necessary for the purpose for which it is obtained (please refer to DPIA Tool in Annex 3 for the data flow/mapping).
7.3.2 All data collection forms (electronic or paper-based), including data collection requirements in new information systems, must be include a fair processing statement or link to privacy statement and approved by the DPO.
7.3.3 The DPO will ensure that, on an annual basis all data collection methods are reviewed by internal audit to ensure that collected personal data continues to be adequate, relevant and not excessive (for further details please see Data

Protection Impact Assessment Procedure in Annex 10 and DPIA Tool in Annex 3).

7.4. Personal data must be accurate and kept up to date with every effort to erase or rectify without delay

7.4.1 Data that is stored by the data controller must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate.

7.4.2 The DPO is responsible for ensuring that all staff are trained in the importance of collecting accurate data and maintaining it.

7.4.3 It is also the responsibility of the data subject to ensure that data controlled by CEU is accurate and up to date. Completion of a registration or application form by a data subject will include a statement that the data contained therein is accurate at the date of submission.

7.4.4 Members of the CEU Community should be required to notify CEU of any changes in circumstance to enable personal records to be updated accordingly. It is the responsibility of the DPO to ensure that any notification regarding change of circumstances is recorded and acted upon.

7.4.5 The DPO 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.

7.4.6 On at least an annual basis, the DPO will review the retention dates of all the personal data processed by CEU by reference to the data inventory, and will identify any data that is no longer required in the context of the registered purpose. This data will be securely deleted/destroyed in line with the Secure Disposal of Storage Media Procedure (Annex 11 – Secure Disposal of Storage Media Procedure).

7.4.7 The DPO is responsible for responding to requests for rectification from data subjects within 25 days, following a proof of identity and change ("Subject Access Request Procedure", please see Annex 6 – Subject Access Request Procedure). The Subject Access Request Procedure can be extended to a further two months for complex requests. If CEU decides not to comply with the request, the DPO must respond to the data subject to explain its reasoning and inform them of their right to complain to the supervisory authority and seek judicial remedy.

7.4.8 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 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.

7.5. Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing

7.5.1 Where personal data is retained beyond the processing date, it will be minimized/encrypted/pseudonymized in order to protect the identity of the data subject in the event of a data breach. For further guidance please refer to Pseudonymisation, Minimization and Encryption Guidance (Annex 12 – Pseudonymisation, Minimization and Encryption Procedure).

7.5.2 Personal data will be retained in line with the Retention of Records Procedure (Annex 13 – Retention of Records Procedure) and, once its retention date is passed, it must be securely destroyed as set out in this procedure.

7.5.3 The DPO must specifically approve any data retention that exceeds the retention periods defined in Retention of Records Procedure (Annex 13), and must ensure that the justification is clearly identified and in line with the requirements of the data protection legislation. This approval must be written.

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

The DPO will carry out a risk assessment taking into account all the circumstances of CEU's controlling or processing operations.

In determining appropriateness, the DPO should also consider the extent of possible damage or loss that might be caused to individuals (e.g. staff or customers) 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 DPO will consider the following:

- Password protection (Annex 14 - User Access Management);
- Automatic locking of idle terminals;
- Removal of access rights for USB and other memory media (Annex 15 - Access Control Rules and Rights for Users & Annex 11 – Secure Disposal of Storage Media);
- Virus checking software and firewalls (Annex 16 – Notebook Computer Security);
- Role-based access rights including those assigned to temporary staff (Annex 15 - Access Control Rules and Rights for Users);
- Encryption of devices that leave the organisations premises such as laptops (Annex 16 - Notebook Computer Security);
- Security of local and wide area networks (Annex 16 - Notebook Computer Security);
- Privacy enhancing technologies such as pseudonymization and anonymization;
- Identifying appropriate international security standards relevant to .

When assessing appropriate organizational measures, the DPO will consider the following:

- The appropriate training levels throughout CEU;
- Measures that consider the reliability of employees (such as references etc.);
- The inclusion of data protection in employment contracts;
- Identification of disciplinary action measures for data breaches;
- Monitoring of staff for compliance with relevant security standards;
- Physical access controls to electronic and paper based records;
- Adoption of a clear desk policy;
- Storing of paper based data in lockable fire-proof cabinets;
- Restricting the use of portable electronic devices outside of the workplace;
- Restricting the use of employee's own personal devices being used in the workplace;
- Adopting clear rules about passwords;
- Making regular backups of personal data and storing the media off-site;
- The imposition of contractual obligations on the importing organisations to take appropriate security measures when transferring data outside the EEA.

These controls have been selected on the basis of identified risks to personal data, and the potential for damage or distress to individuals whose data is being processed.

7.7. The controller must be able to demonstrate compliance with the GDPR's other principles (Accountability)

CEU demonstrates compliance with the data protection principles by having implemented data protection policies, adhering to codes of conduct, implementing technical and organisational measures, as well as adopting techniques such as data protection by design, DPIAs, breach notification procedures and incident response plans.

8. Data Processors

8.1 Where processing is to be carried out on behalf of CEU, CEU shall use only processors providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

8.2 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 by other legal act within the Hungarian Data Protection Act and binding legislation of the European Union, including if the contract was made out by way of electronic means. CEU shall be held liable for the lawfulness of his instructions given to the data processor.

8.3 If a data processor determines, in infringement of the applicable data protection law, the purposes and means of processing, that data processor shall be considered to be a data controller in respect of that processing.

9. Data Subjects' Rights

9.1 Data subjects have the following rights regarding personal data processing, and the personal data that is recorded about them:

- 9.1. 1 To be informed of the circumstances of data processing before the commencement of processing.
- 9.1. 2 To obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed.
- 9.1. 3 To request the data controller to make available his or her personal data and information concerning the processing thereof such as:
  - a) the purposes and the legal basis of the processing
  - b) source and categories of the processed personal data
  - c) the recipients of the personal data and the envisaged period of processing
  - d) the rights of the data subject and the manner in which they can be exercised;
  - e) where profiling is used, an indication thereof;
  - f) the circumstances of any personal data breach that may have occurred in connection with processing the data subject's personal data, their impact, and the measures taken to remedy the situation.
- 9.1. 4 To take action to rectify, restrict, erase, including the right to be forgotten.
- 9.1. 5 To not to 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 process

9.1. 6 To have personal data provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another controller.

9.1. 7 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 Joint Data Controllers, including profiling.

9.1. 8 To request the supervisory authority to assess whether any provision of the GDPR has been contravened.

9.1. 9 To sue for compensation if they suffer damage by any contravention of the GDPR.

9.2 CEU ensures that data subjects may exercise these rights:

9.2. 1 Data subjects may make data access requests as described in Subject Access Request Procedure (Annex 6 – Subject Access Request Procedure); this procedure also describes how CEU will ensure that its response to the data access request complies with the requirements of the GDPR.

9.2. 2 Data subjects have the right to complain to CEU related to the processing of their personal data, the handling of a request from a data subject and appeals from a data subject on how complaints have been handled in line with the Complaints Procedure (Annex 17 – Complaints Procedure).

9.2. 3 The data subject has the right to contact the DPO asking his/her opinion or advice before launching the above-mentioned procedure, as well as to inform him/her about the problem concerning the data processing.

9.2. 4 The contact details of the DPO can be found in CEU's Privacy Notice published at CEU's website.

10. Consent

10.1 CEU understands 'consent' to mean that it has been explicitly and voluntary given, and a specific, informed and unambiguous indication of the data subject's wishes that, by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The data subject can withdraw their consent at any time.

10.2 CEU understands 'consent' to mean that the data subject has been fully informed of the intended processing and has signified the agreement, while in a fit state of mind to do so and without pressure being exerted upon him/her. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing.

10.3 There must be some active communication between the parties to demonstrate active consent (e.g. signed consent form, privacy notice accepted by the data subject before information is being processed, etc.). Consent cannot be inferred from non-response to a communication. The Controller must be able to demonstrate that consent was obtained for the processing operation.

10.4 For sensitive data, explicit written consent (Annex 17 - Complaints Procedure) of data subjects must be obtained unless an alternative legitimate basis for processing exists.

10.5 In most instances, consent to process personal and sensitive data is obtained by CEU using standard consent documents (see Annex 9 – Privacy Notice).

10.6 Where CEU provides online services to children, parental or custodial authorization must be obtained. This requirement applies to children under the age of 16 as follows:

10.6. 1 Person concerned under the age of 14: if the person concerned has not yet reached the age of 14, any of his/her legal representatives (parents) can give his/her consent to the processing of his/her personal data, so the statement that contributes to the processing of the data of the person concerned shall be signed by the legal representative.

10.6. 2 Person concerned between the age of 14 and 16: if the person concerned has reached the age of 14 but has not yet reached the age of 16, the statement that contributes to the processing of the data of the person concerned shall be signed by both the legal representative and the person concerned.

10.6. 3 Person concerned above the age of 16: if the person concerned has reached the age of 16, the prior consent or subsequent approval of his/her legal representative is not required and the person concerned may sign his/her consent for processing his/her personal data.

11. Security of Data

11.1 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.

11.2 All personal data should be accessible only to those who need to use it, and access may only be granted in line with the Access Control Policy (Annex 18 – Access Control Policy). 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
- if computerized, password protected in line with corporate requirements in the Access Control Policy (Annex 18 - Access Control Policy); and/or
- stored on (removable) computer media which are encrypted in line with Secure Disposal of Storage Media (Annex 11 – Secure Disposal of Storage Media Procedure).

11.3 Care must be taken to ensure that PC screens and terminals are not visible except to authorized Members of CEU Community. All Members of CEU Community are required to enter into an Individual User Agreement (Annex 19) before they are given access to organizational information of any sort, which details rules on screen time-outs.

11.4 Manual records (hard copies) may not be left where they can be accessed by unauthorized personnel and may not be removed from CEU's premises without explicit written authorization of the DPO[4]. As soon as manual records are no longer required for day-to-day client support, they must be removed from secure archiving.

11.5 Personal data may only be deleted or disposed of in line with the Retention of Records Procedure (Annex 13 – Retention of Records Procedure). Manual records that have reached their retention date are to be shredded and disposed of as 'confidential waste'. Hard drives of redundant PCs are to be removed and immediately destroyed or deleted as required by Annex 11- Secure Disposal of Storage Media Procedure before disposal.

11.6 Processing of personal data 'off-site' presents a potentially greater risk of loss, theft or damage to personal data.

12. Disclosure of Data

12.1 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.

12.2 CEU may only disclose personal data to the public or unauthorized third parties if:

[4] Please see point 9.2.4 re contact details of theDPO.

- processing is necessary as prescribed by Union law, act or decreed by a local authority based on authorization conferred by act;
- processing is necessary and data subject gave his/her voluntary and explicit consent to CEU.[5]

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

12.4 It is important to bear in mind whether or not disclosure of the information is relevant to, and necessary for, the conduct of CEU's business.

12.5 All requests to provide personal data for one of these reasons must be supported by appropriate paperwork and all such disclosures must be specifically authorized in writing by the DPO.

13. Retention and Disposal of Data

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

13.2 CEU may store 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.

13.3 The retention period for each category of personal data will be set out in the Retention of Records Procedure (Annex 13 – Retention of Records Procedure) along with the criteria used to determine this period including any statutory obligations CEU has to retain the personal data.

13.4 If the duration or periodic review of the need of mandatory data processing is not provided for by an act, municipal decree or binding legislation of the European Union, the data controller shall ensure that an audit of the data processing operations is carried out by a data processor acting on the controller's behalf or following the controller's instructions at least every three years to determine whether it is necessary for the purpose of the data processing. The data controller shall document the circumstances and the outcome of such review and shall keep such document for ten years following the review, and shall make it available to the Authority at the Authority's request.

13.5 CEU's data retention and data disposal procedures (Storage Removal Procedure Annex 11 - Secure Disposal of Storage Media Procedure) will apply in all cases.

13.6 Personal data must be disposed of securely in accordance with the sixth principle of the GDPR – processed in an appropriate manner to maintain security, thereby protecting the

---

12.1 [5] Disclosures do not require consent so long as the information is requested for one or more of the following purposes (not exhaustive list):

- where processing is necessary as prescribed by Union law, act or decreed by a local authority based on authorization conferred by act
- where processing is necessary and proportionate for protecting the vital interests of the data subject or of another person, or in order to prevent or avert an imminent danger posing a threat to the lives, physical integrity or property of persons to safeguard national security;
- where such processing relates to data which are manifestly made public by the data subject and it is necessary and proportionate for the purpose of the data processing
- where processing of sensitive data is strictly necessary and proportionate for the implementation of an international agreement promulgated by an act, or if prescribed by law in connection with the enforcement of fundamental rights afforded by the Fundamental Law, or for reasons of national security or national defence, or law enforcement purposes for the prevention, investigation or prosecution of criminal activities
- prevention or detection of crime including the apprehension or prosecution of offenders;
- assessment or collection of tax duty;
- discharge of regulatory functions (includes health, safety and welfare of persons at work);
- to prevent serious harm to a third party; and
- to protect the vital interests of the individual, this refers to life and death situations.

"rights and freedoms" of data subjects. Any disposal of data will be done in accordance with the secure disposal procedure (Annex 11 - Secure Disposal of Storage Media Procedure).

14. Data Transfers

14.1 All exports of data from within the EEA[6] 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".[7]

14.2 The transfer of personal data outside of the EEA is prohibited unless one or more of the specified safeguards, or exceptions, apply:

14.2.1 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.[8]

14.2.2 Privacy Shield

If CEU wishes to transfer personal data from the EU to an organization in the United States, it should check that the organization is signed up with the Privacy Shield framework at the U.S. Department of Commerce. The obligation applying to companies under the Privacy Shield are contained in the "Privacy Principles". The US DOC is responsible for managing and administering the Privacy Shield and ensuring that companies live up to their commitments. In order to be able to certify, companies must have a privacy policy in line with the Privacy Principles e.g. use, store and further transfer the personal data according to a strong set of data protection rules and safeguards. The protection given to the personal data applies regardless of whether the personal data is related to an EU resident or not. Organizations must renew their "membership" to the Privacy Shield on an annual basis. If they fail to do so, they can no longer receive and use personal data from the EU under that framework.

14.2.3 Binding corporate rules

CEU may adopt approved binding corporate rules for the transfer of data outside the EU. This requires submission to the relevant supervisory authority for approval of the rules that CEU is seeking to rely upon.

14.2.4 Model contract clauses

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.

14.2.5 Exceptions

---

[6] 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.

[7] 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.

[8] 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

In the absence of an adequacy decision, Privacy Shield membership, binding corporate rules and/or model contract clauses, a transfer of personal data to a third country or international organization shall only take place on one of the following conditions:

- the data subject has voluntary and explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
- the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary for the establishment, exercise or defence of legal claims; and/or
- the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.

15. Information Asset Register/Data Inventory

15.1 CEU has established a data inventory and data flow process as part of its approach to address risks and opportunities throughout its GDPR compliance project. CEU's data inventory and data flow determines the following (Annex 10 – Data Protection Impact Assessment Procedure and Annex 3 – DPIA Tool):

- processes that use personal data;
- source of personal data;
- volume of data subjects;
- description of each item of personal data;
- processing activity;
- maintains the inventory of data categories of personal data processed;
- documents the legal basis and the purpose(s) for which each category of personal data is used;
- recipients and potential recipients of the personal data;
- the role of CEU throughout the data flow;
- key systems and repositories;
- any data transfers; and
- all retention and disposal requirements.

15.2 CEU is aware of any risks associated with the processing of particular types of personal data.

15.2.1 CEU assess the level of risk to individuals associated with the processing of their personal data. Data protection impact assessments (DPIAs) (DPIA Procedure GDPR DOC 2.4 and GDPR REC 4.4) are carried out in relation to the processing of personal data by CEU and in relation to processing undertaken by other organizations on behalf of CEU.

15.2.2 CEU shall manage any risks identified by the risk assessment in order to reduce the likelihood of a non-conformance with this Policy.

15.2.3 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.

15.2.4 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.

15.2.5 The DPO shall, if there are significant concerns, either as to the potential damage or distress, or the quantity of data concerned, escalate the matter to the supervisory authority.

15.2.6 Appropriate controls will be selected from Annex A of ISO 27001, and applied to reduce the level of risk associated with processing individual data to an acceptable level, by reference to the requirements of the GDPR.

16. Closing Provisions

16.1 The specific rules related to the processing of personal data are regulated in separate documents attached to this Policy as Annexes.

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

16.3 The present Policy will come into force upon approval by the Senate. Any modification of the Policy requires the approval of the Senate, except of the Annexes.

Budapest, Jauary 21, 2019

Signed by *CEU President and Rector Michael Ignatieff / Aláírta a Közép-európai Egyetem rektora, Michael Ignatieff*

The original document is filed at the Office of the Academic Secretary. / Az eredeti szabályzat az Akadémiai Titkár irodájában található

Annexes:

Annex 1: Information Security Policy
Annex 2: GDPR Objectives Record
Annex 3: DPIA Tool
Annex 4: DPO Job Description
Annex 5: DPO Responsibilities
Annex 6: Subject Access Request Procedure
Annex 7: Training Policy
Annex 8: Privacy Notice Procedure
Annex 9: Privacy Notice
Annex 10: Data Protection Impact Assessment Procedure
Annex 11: Secure Disposal of Storage Media Procedure
Annex 12: Pseudonymisation, Minimisation and Encryption Guidance
Annex 13: Retention of Records Procedure
Annex 14: User Access Management
Annex 15: Access Control Rules and Rights for Users
Annex 16: Notebook Computer Security
Annex 17: Complaints Procedure
Annex 18: Access Control Policy
Annex 19: Individual User Agreement
Annex 20: Subject Access Request Record
Annex 21: Data Subject Consent Withdrawal Form
Annex 22: Withdrawal of Consent Procedure
Annex 23: Retention and Disposal Schedule
Annex 24: Information Security Classification Guidelines
Annex 25: Parental Consent Withdrawal
Annex 26: External Parties: Information Security Procedure
Annex 27: Reporting Weaknesses, Events and Personal Data Breaches Procedure
Annex 28: Schedule of Information Security Event Reports
Annex 29: Responding to Information Security Reports
Annex 30: Personal Data Breach Notification Procedure
Annex 31: Information Security Weaknesses and Events Checklist
Annex 32: Internal Breach Register
Annex 33: Contact With Authorities Work Instruction
Annex 34: Collection of Evidence
Annex 35: Communication Procedure
Annex 36: Treating Personal Data in Research
Annex 37: Organizational Structure

Annex 1
Information Security Policy

The management of CEU are committed to preserving the confidentiality, integrity and availability of all the physical and electronic information assets throughout their organization in order to preserve its competitive edge, cash-flow, profitability, legal, regulatory and contractual compliance and commercial image. Information and information security requirements will continue to be aligned with CEU's goals and the Information Security Policy (ISP) is intended to be an enabling mechanism for information sharing, for electronic operations and for reducing information-related risks to acceptable levels.

In particular, business continuity and contingency plans, data backup procedures, avoidance of viruses and hackers, access control to systems and information security incident reporting are fundamental to this policy. Control objectives for each of these areas are contained in *[location/document/software]* and are supported by specific documented policies and procedures.

CEU aims to achieve specific, defined information security objectives, which are developed in accordance with the business objectives, the context of the organisation, the results of risk assessments and the risk treatment plan.

All Members of CEU Community are expected to comply with this policy. All Faculty and Staff will receive appropriate training. The consequences of breaching the information security policy qualify as Misconduct under CEU's Code of Ethics.

The ISP is subject to continuous, systematic review and improvement.

CEU has established an Information Security Committee (ISC), chaired by the IT Director to periodically review the ISP.

This policy will be reviewed to respond to any changes in the risk assessment or risk treatment plan and at least annually.

In this policy, 'information security' is defined as:

Preserving
This means that management, all Members of CEU Community, sub-contractors, project consultants and any external parties have, and will be made aware of, their responsibilities (which are defined in their job descriptions or contracts) to preserve information security, to report security breaches and to act in accordance with the requirements of the ISMS. All Faculty and Staff will receive information security awareness training and/or specialized information security training.

the availability,

This means that information and associated assets should be accessible to authorized users when required and therefore physically secure. The computer network must be resilient and CEU must be able to detect and respond rapidly to incidents (such as viruses and other malware) that threaten the continued availability of assets, systems and information. There must be appropriate business continuity plans.

confidentiality

This involves ensuring that information is only accessible to those authorized to access it and therefore to preventing both deliberate and accidental unauthorized access to CEU's information and its systems.

and integrity

This involves safeguarding the accuracy and completeness of information and processing methods, and therefore requires preventing deliberate or accidental, partial or complete, destruction or unauthorized modification, of either physical assets or electronic data. There must be appropriate contingency and data backup plans and security incident reporting. CEU must comply with all relevant data-related legislation in those jurisdictions within which it operates.

of the physical (assets)

The physical assets of CEU including, but not limited to, computer hardware, data cabling, telephone systems, filing systems and physical data files.

and information assets

The information assets include information printed or written on paper, transmitted by post or shown in films, or spoken in conversation, as well as information stored electronically on servers, website(s), extranet(s), intranet(s), PCs, laptops, mobile phones and PDAs, as well as on CD ROMs, floppy disks, USB sticks, backup tapes and any other digital or magnetic media, and information transmitted electronically by any means. In this context, 'data' also includes the sets of instructions that tell the system(s) how to manipulate information (i.e. the software: operating systems, applications, utilities, etc).

Of CEU.

A **SECURITY BREACH** is any incident or activity that causes, or may cause, a break down in the availability, confidentiality or integrity of the physical or electronic information assets of CEU.

Annex 2
GDPR Objectives Record

Purpose

Record CEU's objectives for the implementation of the GDPR.

Date	Objective	Document reference	Responsibility	Due date

Annex 3
DPIA Tool

DPIA tool is available in excel format here :
https://ceuedu.sharepoint.com/:x:/r/gdpr/Templates/ANNEX_3_GDPR_REC_4.4.xlsx?d=wc26f14c51eea48299a69de66b501b3af&csf=1&e=XsAHHI

Annex 4
DPO Job Description

Main Purpose

To drive compliance with the EU General Data Protection Regulation (GDPR) and ensure ongoing compliance of all core activities for CEU.

Position

The DPO is a member of the Information Security Committee.

Data protection compliance is a corporate responsibility of the data controller, not of the DPO.

Currently, the Data Protection Officer position ensures the following duties are carried out by (Annex 5 – DPO Responsibilities).

Responsibilities

The DPO will maintain expert knowledge of data protection law and practices, as well as other professional qualities, to ensure that CEU complies with the requirements of the EU GDPR and relevant national data protection law(s) and regulations.

The Data Protection Officer must inform and advise on the protection of personal data in relation to the EU GDPR, national law(s) and regulations as well as CEU's Data Protection Policy.

The Data Protection Officer will ensure that documentation to demonstrate compliance with the GDPR such as policies and procedures are kept up to date. Furthermore, the Data Protection Officer will plan and schedule data processing audits regularly, monitoring core activities to ensure they comply with the EU GDPR.

The Data Protection Officer is the main contact point for employees and will liaise with all Members of CEU Community on matters of data protection.

Key tasks of the Data Protection Officer:

a. To inform and advise all Members of CEU Community on their obligation to adhere to the EU GDPR and national law(s) when dealing with personal data.
b. To monitor compliance with the EU GDPR and national law(s).
c. Advise and inform on the data protection impact assessment (DPIA), including monitoring performance of DPIAs against the requirements of the EU GDPR Article 35.
d. Liaise and cooperate with the supervisory authority.
e. To be the point of contact for the supervisory authority on issues relating to processing of personal data, and to consult with the supervisory authority, where necessary, on any other personal data matters.
f. To contribute to the development and maintenance of all University data protection policies, procedures and processes in relation to the protection of personal data.
g. Advise management on the allocation of responsibilities internally to support ongoing compliance with the EU GDPR and national law(s).
h. Ensure training and awareness is available and delivered to all members of staff involved in processing operations relating to personal data.

i. Regularly monitor compliance with the EU GDPR and national data protection law(s) by conducting audits of processes relating to personal data, and report to the Board of Directors / Chief Executive Officer (CEO) / Top Management.
j. To be the point of contact for data subjects with regard to the processing of their personal data.
k. To monitor compliance with the Data Protection Policy throughout CEU to develop/advise on procedures for effective security.
l. To advise senior management on the allocation of information security responsibilities.
m. To develop/advise on formal procedures for reporting incidents (EU GDPR and information security-related) and investigations under Articles 33 and 34 of the GDPR.
n. To contribute to the business continuity and disaster recovery planning process.
o. To advise on and monitor the safeguarding of organizational record management, (Annex 3).
p. Work with information asset owners to ascertain the extent to which personal data is collected, held and/or used in CEU, and that it is properly controlled and safeguarded from loss of confidentiality, integrity or availability from any cause.
q. To ensure that records of the processing are kept by CEU as detailed in Article 30 mentioned above.
r. To advise the controller of its obligation to issue privacy notices to data subjects at the point of collection of their personal data under Articles 13 to 15.

The Data Protection Officer is authorized to have access to all CEU's systems relating to the collection, processing and storage of personal data for the purpose of assessing the use and security of personal data. The Data Protection Officer may expect the cooperation of all staff in carrying out these duties, including access to systems and records.

Annex 5
DPO Responsibilities

As detailed in your job description, you have been designated the senior management team member accountable to Board of Directors for the management of personal data within Organisation Name. You must ensure that compliance with data protection legislation under the DPA, EU GDPR, any other data protection legislation and good practice can be demonstrated.

GDPR Owner

As detailed in your job description, you have been designated responsible for managing compliance with CEU's data protection policy on a day-to-day basis.

You have the following responsibilities:

a. ensuring implementation of the data protection policy;
b. development and review of the data protection policy;
c. training and ongoing awareness as required by the data protection policy;
d. approval of procedures where personal data is processed, such as:
    i. the management and communication of privacy notices;
    ii. the handling of requests from individuals, including requests for access, rectification, erasure, etc.;
    iii. the collection and handling of personal data;
    iv. complaints handling;
    v. the management of security incidents; and
    vi. outsourcing and off-shoring.
e. liaison with those responsible for risk management and security issues within CEU;
f. provision of expert advice and guidance on legislative and regulatory data protection matters;
g. the interpretation and application of the various exemptions applicable to the processing of personal data;
h. advise and inform on the data protection impact assessment and monitor performance against the requirements of the EU GDPR;
i. provision of advice in relation to data sharing projects (including security issues when data are off site);
j. CEU has access to legislative updates and appropriate guidance related to data protection legislation;
k. continually checking that University's data protection regime reflects changes in legislation, practice and technology;
l. completing, submitting and managing notifications to the supervisory authority where required under the GDPR and other data protection regulations; and
m. implementing, as appropriate, the practices related to the processing of personal data outlined in any mandatory or advisory sectoral codes that apply to CEU.

Data protection representatives/information asset owners

As detailed in your job description, you have been designated a data protection representative, which means that you are required to:

a. represent departments or systems that are recognised as high-risk in relation to the management of personal data;
b. be member of the information governance committee; and

c. assist the GDPR Owner with day-to-day responsibility for compliance with the data protection policy, for example: data inventory, staff training and staff access, privacy notices, privacy impact assessments, etc.

Annex 6
Subject Access Request Procedure

1. Scope

All personal data processed by CEU is within the scope of this procedure. Data subjects shall have the right to access their personal data so that they are aware of and can verify the lawfulness of the processing.

Data subjects are entitled to obtain:

- Confirmation as to whether CEU is processing any personal data about that individual;
- Access to their personal data;
- Any related information;
- The logic involved in any automated decisions relating to him or her.

2. Responsibilities

The DPO is responsible for the application and effective working of this procedure, and for reporting to the information owner.
The DPO is responsible for handling all Subject Access Request Procedure (SARs).

3. Procedure

3.1 Subject Access Requests are made using the Subject Access Request Record (Annex 20 - Subject Access Request Record)

3.2 The data subject provides CEU with evidence of his/her identity, in the form of a current ID/passport, and the signature on the identity must be cross-checked to that on the application form (Annex 20 - Subject Access Request Record).

3.3 The data subject specifies to CEU specific set of data held by CEU on their subject access request (SAR). The data subject can request all data held on them.

3.4 CEU records the date that the identification checks were conducted and the specification of the data sought.

3.5 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. The controller shall inform 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 form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

3.6 Once received, the subject access request (SAR) application is immediately forwarded to the DPO who will ensure that the requested data is collected within the specified time frame in clause 3.4 above.
Collection entails:

3.6.1 Collecting the data specified by the data subject, or

3.6.2 Searching all databases and all relevant filing systems (manual files) at CEU, including all back up and archived files (computerized or manual) and all email folders and archives. The DPO maintains a data map (Inventory) that identifies where all data within CEU is stored.

3.7 The Data Protection Officer maintains a record of requests for data and of its receipt, including dates.

3.8 The Data Protection Officer reviews subject access requests from a child.

3.9 The Data Protection Officer reviews all documents that have been provided to identify whether any third parties are present in it, and either removes the identifying third party information from the documentation or obtains written consent from the third party for their identity to be revealed.

3.10 If any of the requested data is being held or processed under one of the following exemptions, it does not have to be provided:

- National security
- Crime and taxation
- Health
- Education
- Social Work
- Regulatory activity
- Journalism, literature and art
- Research history, and statistics
- Publicly available information
- Corporate finance
- Examination marks
- Examinations scripts
- Domestic processing
- Confidential references
- Judicial appointments, honors and dignities
- Crown of ministerial appointments
- Management forecasts
- Negotiations
- Legal advice and proceedings
- Self-incrimination
- Human fertilization and embryology
- Adoption records
- Special educational needs
- Parental records and reports

3.11 In the event that a data subject requests CEU to provide him/her with the personal data stored by the controller/processor, then CEU will provide the data subject with the requested information in electronic format, unless otherwise specified.

3.12 In the event that a data subject requests what personal data is being processed then CEU provides the data subject with the following information:

3.12.1 Purpose of the processing

3.12.2 Categories of personal data

3.12.3 Recipient(s) of the information, including recipients in third countries or international organizations

3.12.4 How long the personal data will be stored

3.12.5 The data subject's right to request rectification or erasure, restriction or objection, relative to their personal data being processed.

3.12.5.1 CEU removes personal data from systems and processing operations as soon as a request for erasure has been submitted by the data subject.

3.12.5.2 CEU contacts and communicates with other organizations, where the personal data of the data subject is being processed, to cease processing information at the request of the data subject.

3.12.5.3 CEU makes all necessary measures without undue delay in the event that the data subject has: withdrawn consent; objects to the processing of their personal data in whole or part; no longer under legal obligation and/or has been unlawfully processed.

3.12.6 Inform the data subject of their right to lodge a complaint with the supervisory authority and a method to do so (Complaints Procedure, Annex 17).
3.12.7 Information on the source of the personal data if it hasn't been collected from the data subject.
3.12.8 Inform the data subject of any automated decision-making.
3.12.9 If and where personal data has been transferred and information on any safeguards in place.

Annex 7
Training Policy

1. Scope

This policy applies to CEU's training and awareness programme where relevant to the GDPR, compliance with the GDPR, and other matters relating to data protection and privacy.

2. Training policy

2.1 Data Protection Officer assigns data protection responsibilities of Members of CEU Community in relation to CEU's policies and procedures on personal data management.
2.2 Data Protection Officer shall ensure that all Members of CEU Community with day-to-day responsibilities involving personal data and processing operations, and those with permanent/regular access to personal data, demonstrate compliance with the GDPR.
2.3 These members of Employees/Staff are able to demonstrate competence in their understanding of the GDPR *[, best practice and BS 10012:2017 privacy requirements]*, how this is practised and implemented throughout Organisation Name.
2.4 Data Protection Officer ensures that these Members of CEU Community are kept up to date and informed of any issues related to personal data.
2.5 Data Protection Officer maintains a list of relevant external bodies, including the relevant national supervisory authority.
2.6 The management of CEU promotes training and awareness programmes, and CEU shall make resources available in order to raise awareness. The Data Protection Officer shall demonstrate and communicate to Members of 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.
2.7 Data Protection Officer ensures that all security requirements related to data protection are demonstrated and communicated to all Members of CEU Community to the same affect.
2.8 Members of CEU Community are provided with specific training on processing personal data relevant to their individual day-to-day roles and responsibilities, and in accordance with CEU's policies and procedures.
2.9 Members of CEU Community are provided with specific training on any information security requirements and procedures applicable to data protection and the data processing within their individual day-to-day roles and responsibilities, including reporting personal data breaches.
2.10 Faculty and Staff are provided with training on dealing with complaints relating to data protection and processing personal data.
2.11 The Data Protection Officer retains records of the relevant training undertaken by each person who has this level of responsibility.
2.12 The Data Protection Officer is responsible for organising relevant training for all responsible individuals and Faculty and Staff generally, and for maintaining records of the attendance of staff at relevant training at appropriate times CEU's operational cycle.

Annex 8
Privacy Procedure

1. Scope

All processing of personal data by CEU is within the scope of this procedure.

2. Responsibilities

2.1 The Data Protection Officer is responsible for ensuring that the privacy notice(s) is correct and that mechanisms exist such as having the Privacy Notice(s) on CEU's website to make all data subjects aware of the contents of this notice prior CEU commencing collection of their data.

2.2 Members of CEU Community that need to collect personal data are required to follow this procedure.

3. Procedure

3.1 CEU identifies the **legal basis** for processing personal data before any processing operations take place by clearly establishing, defining and documenting:

- 3.1.1 the specific purpose of processing the personal data and the legal basis to process the data under:
  - 3.1.1.1 consent obtained from the data subject;
  - 3.1.1.2 performance of a contract where the data subject is a party;
  - 3.1.1.3 legal obligation that CEU is required to meet;
  - 3.1.1.4 protect the vital interests of the data subject, including the protection of rights and freedoms;
  - 3.1.1.5 official authority of CEU or to carry out the processing that is in the public interest;
  - 3.1.1.6 necessary for the legitimate interests of the data controller or third party, unless the processing is overridden by the vital interests, including rights and freedoms;
  - 3.1.1.7 national law.
- 3.1.2 any special categories of personal data processed and the legal basis to process the data under:
  - 3.1.2.1 explicit consent obtained from the data subject;
  - 3.1.2.2 necessary for employment rights or obligations;
  - 3.1.2.3 protect the vital interests of the data subject, including the protection of rights and freedoms;
  - 3.1.2.4 necessary for the legitimate activities with appropriate safeguards;
  - 3.1.2.5 personal data made public by the data subject;
  - 3.1.2.6 legal claims;
  - 3.1.2.7 substantial public interest;
  - 3.1.2.8 preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, provision of health or social care treatment, or management of health and social care systems and services, under the basis that appropriate contracts with health professionals and safeguards are in place;
  - 3.1.2.9 public health, ensuring appropriate safeguards are in place for the protection of rights and freedoms of the data subject, or professional secrecy;
  - 3.1.2.10 national laws in terms of processing genetic, biometric or health data.

3.2 CEU records this information in line with its data protection impact assessment and data inventory (Annex 10 and Annex 3).

4. Privacy Notices

4.1 When personal data collected from data subject with consent

4.1.1 CEU is transparent in its processing of personal data and provides the data subject with the following:

4.1.1.1 CEU's identity, and contact details of the Data Protection Officer and any data protection representatives;

4.1.1.2 The purpose(s), including legal basis, for the intended processing of personal data (clause 4.2 below);

4.1.1.3 Where relevant, CEU's legitimate interests that provide the legal basis for the processing;

4.1.1.4 Potential recipients of personal data;

4.1.1.5 Any information regarding the intention to disclose personal data to third parties and whether it is transferred outside the EU. In such circumstances, CEU will provide information on the safeguards in place and how the data subject can also obtain a copy of these safeguards;

4.1.1.6 If CEU is based outside of the EU and the data subject resides within it (the EU), CEU provides the data subject with contact details of a data protection representative in the EU;

4.1.1.7 Any information on website technologies used to collect personal data about the data subject;

4.1.1.8 Any other information required to demonstrate that the processing is fair and transparent.

4.1.2 All information provided to the data subject is in an easily accessible format (PDF, printed letter, or email), concise, transparent, intelligible using clear and plain language, especially for personal data addressed to a child.

4.1.3 CEU facilitates the data subject's rights in line with the data protection policy and the subject access request procedure (Annex 6).

4.1.4 Privacy notice for this personal data processing is recorded (Annex 9)

4.2 When data is contractually required for processing

4.2.1 CEU processes data without consent in order to fulfil contractual obligations.

4.2.2 Privacy notice for this personal data processing is recorded (Annex 9)

4.3 When personal data has been obtained from a source other than the data subject

4.3.1 CEU makes clear the types of information collected as well as the source of the personal data (publicly accessible sources) and provides the data subject with:

4.3.1.1 CEU's (data controller) identity, and contact details of the Data Protection Officer and any data protection representatives;

4.3.1.2 The purpose(s), including legal basis, for the intended processing of personal data;

4.3.1.3 Categories of personal data;

4.3.1.4 Potential recipients of personal data;

4.3.1.5 Any information regarding disclosing personal data to third parties and whether it is transferred outside the EU – Organisation Name will provide information on the safeguards in place and how the data subject can also obtain a copy of these safeguards;

4.3.1.6 Any other information required to demonstrate that the processing is fair and transparent.

4.3.2 Privacy notice for this personal data processing is recorded (GDPR REC 4.1)

5. Timing

5.1 CEU provides the information stated in clauses 3 and 4 above within:

5.1.1 one month of obtaining the personal data, in accordance with the specific circumstances of the processing;

5.1.2 at the first instance of communicating in circumstances where the personal data is used to communicate with the data subject;

5.1.3 when personal data is first disclosed in circumstances where the personal data is disclosed to another recipient.

6. Exemptions

6.1 Clauses 3 and 4 above do not apply:

6.1.1 If the data subject already has the information;

6.1.2 If the provision of the above information proves impossible or would involve an excessive effort;

6.1.3 If obtaining or disclosure of personal data is expressly identified by Member State law; or

6.1.4 If personal data must remain confidential subject to an obligation of professional secrecy regulated by national law, including a statutory obligation of secrecy.

Annex 9
Privacy Notice

1. Scope

All data subjects whose personal data is collected, in line with the requirements of the GDPR.

2. Responsibilities

2.1 The Data Protection Officer is responsible for ensuring that this notice is made available to data subjects prior to CEU collecting/processing their personal data.

2.2 Members of CEU Community who interact with data subjects are responsible for ensuring that this notice is drawn to the data subject's attention and their consent to the processing of their data is secured.

3. Privacy notice

3.1 Who are we?

[This needs to be like an executive summary. Identify who we are as an organisation, what we do etc.]

Our Data Protection Officer can be contacted directly here:

- (dpo@ceu.edu)
- (phone:)

The personal data we would like to *[collect from/process on]* you is:

Personal data type:	**Source** (where CEU obtained the personal data from if it has not been collected directly from you, the data subject. Note if the personal data has been accessed from publicly accessible sources):

The personal data we collect will be used for the following purposes:

-
-
-

Our legal basis for processing for the personal data:

-
-
-

Any legitimate interests pursued by us, or third parties we use, are as follows:

-
-
-

The special categories of personal data concerned are:

- Racial
- Ethnic origin
- Political opinions
- Religious beliefs
- Philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data
- Health data
- Data concerning a natural person's sex life
- Sexual orientation
- Other

3.2 **[Consent**

By consenting to this privacy notice you are giving us permission to process your personal data specifically for the purposes identified.
Consent is required for CEU to process both types of personal data, but it must be explicitly given. Where we are asking you for sensitive personal data we will always tell you why and how the information will be used.

You may withdraw consent at any time (please see Annex 22).][9]

3.3 **Disclosure**

CEU will not pass on your personal data to third parties without first obtaining your consent unless there is a legal requirement to do so. *[The following third parties will receive your personal data for the following purpose(s) as part of the processing activities:]*

Third country (non-EU)/international organization	**Safeguards in place to protect your personal data**	**Retrieve a copy of the safeguards in place here:**
Organization Name & geographic location		

3.4 **Retention period**

CEU will process personal data for *[state how long you intend to process the data subject's personal data]* and will store the personal data for *[state the retention period of their personal data and provide further information on how the retention period has been established. Refer to Annex 13 Retention Period Procedure]*.

3.5 **Your rights as a data subject**

[9] When consent is not needed for processing personal data (e.g. when processing is based on the legal basis, incl. legitimate interest, legal obligation, etc. as determined in point 6.1, (a) – (f) of the Data Protection Policy), please delete this part.

At any point while we are in possession of or processing your personal data, you, the data subject, have the following rights:

- Right of access – you have the right to request a copy of the information that we hold about you.
- Right of rectification – you have a right to correct data that we hold about you that is inaccurate or incomplete.
- Right to be forgotten – in certain circumstances you can ask for the data we hold about you to be erased from our records.
- Right to restriction of processing – where certain conditions apply to have a right to restrict the processing.
- Right of portability – you have the right to have the data we hold about you transferred to another organisation.
- Right to object – you have the right to object to certain types of processing such as direct marketing.
- Right to object to automated processing, including profiling – you also have the right to be subject to the legal effects of automated processing or profiling.
- Right to judicial review: in the event that CEU refuses your request under rights of access, we will provide you with a reason as to why. You have the right to complain as outlined in clause 3.6 below.

All of the above requests will be forwarded on should there be a third party involved (as stated in 3.4 above) in the processing of your personal data.

3.6 **Complaints**

In the event that you wish to make a complaint about how your personal data is being processed by CEU (or third parties as described in 3.4 above), or how your complaint has been handled, you have the right to lodge a complaint directly with the supervisory authority and CEU's data protection representatives Data Protection Officer.

The details for each of these contacts are:

	Supervisory authority contact details	**DPO contact details**
Contact Name:		
Address line 1:		
Address line 2:		
Address line 3:		
Address line 4:		
Address line 5:		
Email:		
Telephone:		

3.7 **Privacy statement**

Read more about how and why we use your data here *[provide a link to your privacy statement on the website]*.

4. [Online privacy statement

Personal data

Under the EU's General Data Protection Regulation (GDPR) personal data is defined as:

> "any information relating to an identified or identifiable natural person ('data subject'); 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".

How we use your information

This privacy notice tells you how we, Central European University will collect and use your personal data for *[outline further information on services and activities that you collect personal data, for example: cookies, profiling, complaints, subscriptions, etc.)]*

Why does CEU need to collect and store personal data?

In order for us to provide you *[with a service]* we need to collect personal data for *[correspondence purposes and/or detailed service provision]*. In any event, we are committed to ensuring that the information we collect and use is appropriate for this purpose, and does not constitute an invasion of your privacy.

Will CEU share my personal data with anyone else?

We may pass your personal data on to third-party service providers contracted to CEU in the course of dealing with you. Any third parties that we may share your data with are obliged to keep your details securely, and to use them only to *[fulfil the service they provide you on our behalf]*. When they no longer need your data to fulfil this service, they will dispose of the details in line with CEU's procedures. If we wish to pass your sensitive personal data onto a third party we will only do so once we have obtained your consent, unless we are legally required to do otherwise.

How will CEU use the personal data it collects about me?

CEU will process (collect, store and use) the information you provide in a manner compatible with the EU's General Data Protection Regulation (GDPR). We will endeavor to keep your information accurate and up to date, and not keep it for longer than is necessary. CEU is required to retain information in accordance with the law, such as information needed for income tax and audit purposes. How long certain kinds of personal data should be kept may also be governed by specific business-sector requirements and agreed practices. Personal data may be held in addition to these periods depending on individual business needs.

Under what circumstances will CEU contact me?

Our aim is not to be intrusive, and we undertake not to ask irrelevant or unnecessary questions. Moreover, the information you provide will be subject to rigorous measures and procedures to minimize the risk of unauthorized access or disclosure.

Can I find out the personal data that the organization holds about me?

CEU at your request, can confirm what information we hold about you and how it is processed. If CEU does hold personal data about you, you can request the following information:

- Identity and the contact details of the person or organisation that has determined how and why to process your data. In some cases, this will be a representative in the EU.
- Contact details of the data protection officer, where applicable.
- The purpose of the processing as well as the legal basis for processing.
- If the processing is based on the legitimate interests of CEU or a third party, information about those interests.
- The categories of personal data collected, stored and processed.
- Recipient(s) or categories of recipients that the data is/will be disclosed to.
- If we intend to transfer the personal data to a third country or international organisation, information about how we ensure this is done securely. The EU has approved sending personal data to some countries because they meet a minimum standard of data protection. In other cases, we will ensure there are specific measures in place to secure your information.
- How long the data will be stored.
- Details of your rights to correct, erase, restrict or object to such processing.
- Information about your right to withdraw consent at any time.
- How to lodge a complaint with the supervisory authority.
- 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 you are obliged to provide the personal data and the possible consequences of failing to provide such data.
- The source of personal data if it wasn't collected directly from you.
- Any details and information of automated decision making, such as profiling, and any meaningful information about the logic involved, as well as the significance and expected consequences of such processing.

What forms of ID will I need to provide in order to access this?

CEU accepts the following forms of ID when information on your personal data is requested: ID, Passport, driving license.

Contact details of the Data Protection Officer:

	DPO contact details
Contact Name:	
Address line 1:	
Address line 2:	
Address line 3:	
Address line 4:	

Address line 5:	
Email:	
Telephone:	

Annex 10
Data Protection Impact Assessment Procedure

1. Scope

All projects that involve processing personal data, or any activities (both internal and external) that affect the processing of personal data and impact the privacy of data subjects are within the scope of this procedure and will be subject to a data protection impact assessment (DPIA).

2. Responsibilities

2.1 The Data Protection Officer is responsible for performing necessary checks on personal data to establish the need for conducting a DPIA (please refer to screening questions in Annex 3).

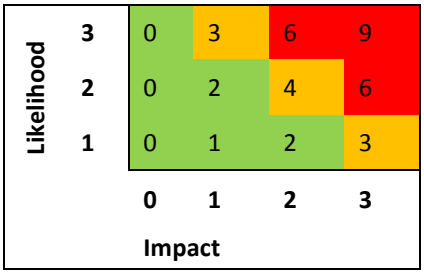
2.2 The Data Protection Officer is responsible for checking appropriate controls are implemented to mitigate any risks identified as part of the DPIA process and subsequent decision to proceed with the processing.

3. Procedure

3.1 The Data Protection Officer identifies the need for a DPIA at the start of each project, assessing the project and type of personal data involved, or processing activity, against the screening questions set out in the DPIA tool (Annex 3).

3.2 Using the criteria below, following the likelihood and impact matrix, CEU defines the risks to rights and freedoms of data subjects as (Annex 3):

Likelihood and impact matrix:



Risks to rights and freedoms of data subjects:

Risk Level	From	To	GDPR Assessment
High	6	9	Highest unacceptable risk
Medium	3	5	Unacceptable risk
Low	1	2	Acceptable risk
Zero	0	0	No risk

4. Data processing workbook (data flow)

4.1 CEU records key information about all personal data processed for each project in the DPIA Tool workbook (Annex 3). This includes a description of the processing and purposes; legitimate interests pursued by the controller; an assessment of the necessity and proportionality of the processing; an assessment of the risks to the rights and freedoms of data subjects (as per the matrix and risk level definitions in clause 3.2 above).

4.2 CEU captures the type of processing activity associated with the personal data being processed as part of the project in the DPIA Tool workbook (Annex 3). These are categorised as:

- Collection
- Transmission
- Storage
- Access
- Deletion

4.3 CEU establishes on what lawful basis the data is being processed and its appropriate retention period (in line with Retention of Records Procedure, Annex 13).

4.4 CEU identifies the category of data processed, whether it is personal, special or that of a child's, and the format of the data.

4.5 CEU identifies who has access to the data (individuals, teams, third-parties or data processor) or who are involved in the processing of personal data, or processing activity, recording the geographic location of where the processing takes place and / or if it is transborder processing.

5. Identify privacy risks

5.1 CEU assesses the privacy risks for each process activity as described in clause 3 above by:

5.1.1 Identifying and describing the privacy risk associated to that process activity

5.1.2 Using the likelihood criteria (1 – low, 2 – medium and 3 - high), scoring the likelihood of the risk occurring

5.1.3 Using the impact criteria (0 – zero impact, 1 – low, 2 – medium and 3 - high) of the risk should it occur

5.1.4 Producing a calculated risk, identifying the risk to the rights and freedoms of data subjects.

5.2 In assessing the privacy risks, CEU considers: risks to the rights and freedoms of natural persons resulting from the processing of personal data; risks to the business (including reputational damage); and its objectives and obligations (both regulatory and contractual).

5.3 CEU identifies solutions to privacy risks, assigns a risk treatment owner and sets a target date for completion.

5.4 CEU prioritises analysed risks for risk treatment based on the risk level criteria established in clause 3.2 above.

5.5 CEU risk owner, in consultation with Data Protection Officer, approves and signs off each DPIA for each data processing activity.

6. Prior consultation

6.1 Where the DPIA identifies that processing of personal data will result in high risk to the data subject, in the absence of risk mitigating measures and controls, CEU consults with the supervisory authority *[at this location]*, using the following method.

6.2 When CEU requests consultation from the supervisory authority it provides the following information:

- 6.2.1 detail of the responsibilities of CEU *([controller/processor/joint controller]*), and the *[data controller/processor/joint controller]* involved in the processing;
- 6.2.2 purpose of the intended processing;
- 6.2.3 detail of any/all measures and controls in place/provided to protect the rights and freedoms of the data subject(s);
- 6.2.4 contact details of the Data Protection Officer as recorded *[where]*;
- 6.2.5 a copy of the data protection impact assessment; and
- 6.2.6 any other information requested by the supervisory authority.

Please note that the supervisory authority may request more information.

Annex 11
Secure Disposal of Storage Media Procedure

1. Scope

CEU requires that all removable storage media are clean (which means it is not possible to read or reconstitute the information that was stored on the device or document) prior to disposal.

2. Responsibilities

2.1 The IT Director is responsible for managing the secure disposal [ISO27002 Clauses 8.3.2 11.2.7] of all storage media in line with this procedure when they are no longer required.

2.2 All owners of removable storage media are responsible for ensuring that these media are disposed of in line with this procedure.

3. Procedure

3.1 Hard disks must be cleared of all software and all organizational confidential and restricted information prior to disposal or reuse, as set out in Clause 3.5 and 3.6, below.

3.1.1 In the event that hard disks/media contain personal data, and it cannot be removed, then:

3.1.1.1 Review whether or not you really do need to keep an archive within which this personal data is stored; it may well be that there is no overriding business reason for the archive in the first place.

3.1.1.2 If you currently cannot technically delete archived data that is beyond its retention date, then to the hard disk/media needs to be put securely beyond use.

3.2 The IT Director is responsible for the secure disposal of storage media and the disposal of all information processing equipment is routed through their office. The information asset inventory and/or data inventory is adjusted once the asset has been disposed of.

3.3 Hard disks are cleaned using *[insert details of technology and process]* and *[insert details of any process used to verify that they have been cleaned]*.

3.4 Hard disks are cleaned by *[insert details of external service provider]* who guarantee *[insert details of level of cleaning and process used for verification]*.

3.5 Devices containing confidential information *[dependent on a risk assessment]* are destroyed *[how?]* prior to disposal and are never reused.

3.6 Devices containing confidential information that are damaged are subject to a risk assessment prior to sending for repair, to establish whether they should be repaired or replaced.

3.7 Portable or removable storage media of any description are destroyed *[how?]* prior to disposal.

3.8 All media are disposed of in line with *[local jurisdictional]* regulations *[which are what?]* on disposal of computer equipment, through CEU's approved contractor *[who?].*

3.9 Documents containing confidential and restricted information that are to be destroyed are shredded by their *[owners]*, using a shredder with an appropriate security classification. These shredders are located *[where?]*. The waste is removed by the approved contractor.

Annex 12
Pseudonymisation, Minimisation and Encryption Guidance

The GDPR refers to a number of data protection terms such as pseudonymisation, minimisation and encryption.

These are discussed briefly in turn.

Pseudonymisation

Pseudonymising personal data can reduce the risks to data subjects and help controllers and processors meet their data protection obligations by ensuring that the additional information that attributes personal data to a specific data subject is kept separately.
The GDPR defined pseudonymisation as "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."

An example of pseudonymised data is as follows:

In Table 1 it is easy to identify each of the data subjects by Data Subject#, First Name & Last Name.
Tables 2 and 3 provide additional information about Data Subject 3 but because they are held separately and segregated from each other, it is not possible to identify the 'natural person'.

Table 1:

Data Subject #	First Name	Last Name
1	Fred	Jones
2	Albert	Einstein
3	Erin	Brockovic
4	John	Lewis

Table 2:

Data Subject #	Sex	Age
3	F	55

Table 3:

Data Subject #	Patient ID	Practice Address 1	Practice Address 2	Practice Address 3	Practice Post Code
3	101234	The Surgery	Somewhere St	Anyplace	LL65 3NY

Minimization

Data minimization applies to the third principle of data protection introduced by the Data Protection Directive 95/46/EC and has been incorporated into the GDPR.

The third principle of data protection specifies that personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

This obliges data controllers to obtain and use only those pieces of information that are necessary for the data controller's purpose(s) for processing such information. Holding any additional personal data on individuals is unlawful.

Encryption

You will need to determine whether your mobile devices need to have their hard drives encrypted. As a matter of good practice, any device with personal data stored on it should use encryption to protect this data.

1. The UK Information Commissioner's approach to encryption of mobile devices is described, on their website, thus:

   By their very nature mobile devices such as laptops, smartphones and tablets have a high risk of loss or theft. Encryption of the data contained on the device can provide an assurance that, if this happens, the risk of unauthorized or unlawful access is significantly minimized.

   Non-mobile devices, such as desktop PCs and servers, have a lower risk of loss or theft when they are stored and used in a secure location, eg, in a server room with restricted access. Although encryption is not generally used in non-mobile devices, data controllers should recognize that there is still a risk of loss or theft of a disk or the device itself (e.g. during a break-in). Therefore, using encryption on non-mobile devices can be beneficial especially when the physical security cannot be maintained at an appropriate level.

2. Laptop whole-disk encryption

   Sensitive and personal information that is on a laptop must, clearly, be encrypted. Of course, any other confidential information – financial data, customer information, and so on – should also be encrypted to protect it if the laptop is ever lost or stolen. The drawback with encryption solutions that only encrypt those files that contain confidential information is that laptop users don't always ensure they always save data into these folders, and these encryption solutions do not automatically encrypt temporary files or caches.

   As a result, and in order to reduce exposure, many organizations are turning to **whole-disk encryption** (also called full-disk encryption) and are looking for solutions that will automatically encrypt any portable storage media – such as USB sticks and CD-ROMs – to which encrypted data might be exported.

   Apart from FIPS-compliance, key factors that should be taken into account when assessing a full-disk encryption product are as follows:

   - Ease of use: the solution should be straightforward and easy to deploy, should require authentication at boot-up, and should require some form of two-factor authentication.
   - End-user productivity: the encryption functionality should not interfere with or reduce end-user productivity; after initial encryption of the disk, all subsequent encryption/decryption should be performed 'on-the-fly' while allowing users to continue working.
   - Ability to encrypt portable storage media, as well as files stored to shared drives and/or in files and directories shared with others.
   - Encrypted data needs to be accessible as part of the business continuity planning process, and this includes an option for recovering from a lost token or forgotten password.

- Enterprise systems integration: while this is particularly important to larger organisations, central management, administration and helpdesk support – as well as integration with existing authentication processes, directories and systems – are all important to the effective roll out of an encryption solution.

3. Documentation

   The requirement that laptops are encrypted and that users do nothing to undermine the effectiveness of the encryption software – and protect any cryptographic keys or authentication devices – should be written into user access agreements.
   CEU's chosen configuration requirements for its encryption software solution should be documented, and the maintenance of this configuration standard should be subject to regular monitoring and technical checking.

Annex 13
Retention of Records Procedure

1. Scope

All CEU's records, whether analogue or digital, are subject to the retention requirements of this procedure.

2. Responsibilities

2.1 The following roles are responsible for retention of these records because they are the information asset owners.
2.2 Asset owners are/responsible for ensuring that all personal data is collected, retained and destroyed in line with the requirements of the GDPR.
2.3 The CFO is responsible for retention of financial (accounting, tax) and related records.
2.4 The HRO is responsible for retention of all HR records.
2.5 The Data Protection Officer is responsible for storage of data in line with this procedure.
2.6 The management of CEU is responsible for ensuring that retained records are included in business continuity and disaster recovery plans.

3. Procedure

3.1 The required retention periods, by record type, are recorded in (Retention of Records, Annex 23) under the following categories:
  3.1.1 Record type
  3.1.2 Retention period
  3.1.3 Retention period to start from (at creation, submission, payment, etc.)
  3.1.4 Retention justification
  3.1.5 Record medium
  3.1.6 Disposal method
3.2 Each data asset that is stored is marked *[how and by whom]* with the name of the record, the record type, the original owner of the data, the information classification (please see Annex 24), the data of storage, the required retention period, the planned date of destruction, and any special information (e.g. in relation to cryptographic keys).
3.3 Cryptographic keys, which are required for *[identify record types above]* are retained.
3.4 For all storage media (electronic and hard copy records), University retains *[specify where and how]* the means to access that data.
3.5 For all electronic storage media, University does not exceed [90%] of the manufacturer's recommended storage life. This is recorded in the Log of Information Assets for Disposal (Annex 11). When the maximum of *[90% of expected life]* is reached, the stored data is copied onto new storage media. *[Here is the work instruction for how this is done]*.
3.6 The procedure for accessing stored data is detailed in Access Control Rules and Rights for Users/User Group (Annex 15) *[insert here how access should be authorized and mechanically affected and how records are protected from loss, destruction or falsification during this process]*.
3.7 The Data Protection Officer is responsible for destroying data once it has reached the end of the retention period as specified in Retention and Disposal Schedule (Annex 23). Destruction must be completed within *[30 days]* of the planned retention period. Destruction is handled as follows: *[insert details of how, by information classification and media, each type of retained record is to be destroyed]*.
3.8 Portable/removable storage media are destroyed in line with Annex 11.

Annex 14
User Access Management

1. Scope

The access rights of all users/user groups (as specified in Annex 15) to any of CEU's information assets, systems or services are managed in accordance with this procedure. CEU operates a single sign-on process *[details] [or, if you don't, this would be the spot to describe the different sign-on requirements by system]*.

2. Responsibilities

2.1 The IT Director is responsible for administration of allocated and authorised user/user group access rights in conformity with the policy.
2.2 The IT Director is responsible for initiation and administration of new and changed user access requests (user agreements) and user training.
2.3 Manager/Executive are responsible for authorising access requests as being in line with business and organisational security policy and procedure.
2.4 Asset owners are responsible for authorising access requests to their information assets as being in conformity to the security requirements of the asset.
2.5 The IT Director is responsible for reviewing user access rights in line with the review requirements of the GDPR.

3. User registration and de-registration

3.1 User agreements contain statements of access rights and statements indicating that users have understood and accepted the conditions of access. CEU's standard User Agreement template is Annex 19.
3.2 Every user's proposed access rights are documented in a User Agreement, which details the systems/services/applications/information assets to which access is to be granted, together with the level of access that is to granted, taking into account the Access Control Policy (Annex 18) and the standard user profiles set out in Annex 15. If a user is to be granted access rights other than the standard ones set out in GDPR-C DOC 9.1.2, then the specific additional authorisation of the IT Director is also required.
3.3 The Manager/Executive and the system/asset owner authorise access to the system/asset.
3.4 The User Agreement is then signed by the user and passed to the IT Director and the username/user ID is created and administered.
3.5 The IT Department maintains a list of authorised users, administers changes in access rights and removes users.
3.6 The Code of Ethics will be invoked in cases of attempted unauthorised access.

4. Privilege management

4.1 Privileges are allocated to a different username than that allocated for normal use.
4.2 The available access privileges for each of CEU's operating systems, applications and other systems, are identified and documented in Annex 15.
4.3 Privileges are allocated on a need-to-use and event-by-event basis; the request for allocation of a privilege is initiated in an e-mail from the user concerned to the IT Director which sets out the reasons why the privilege is required and the length of time for which it is required.
4.4 The IT Director retains a log of all privileges authorised and allocated and checks on a *monthly* basis that they have been de-activated as specified in the original request.

4.5 The IT Director checks *[how?] [on a monthly basis]* that unauthorised privileges have not been obtained.

5. Password management

5.1 The allocation of passwords is formally controlled, as set out in *this policy*.
5.2 User password responsibilities are documented in their signed User Agreements (Annex 19).
5.3 Users are initially issued with a unique temporary password which they are forced to change at first logon.
5.4 *[yearly]* password changes are enforced, re-use of passwords is prohibited for ten subsequent attempts, and twelve-character alphanumeric passwords are required.
5.5 Users who need to be issued with a replacement password IT Department must first obtain the written authorisation of their Manager/Executive (who is required to confirm the identity of the user); this written authorisation must be presented to the before a new unique temporary password can be issued.
5.6 Passwords are stored on CEU's domain controllers are stored separately from application system data.
5.7 The default passwords on all new equipment are changed to conform with CEU's password requirements (Annex 19) before the equipment is brought into service.

6. Review of user access rights

6.1 Access rights are reviewed *yearly* and their adequacy is confirmed; any changes that need to take place are actioned.
6.2 User access rights are reviewed when a user's role or location within CEU changes in any way. If the access rights need to change, a new user agreement is issued, in line with this procedure, setting out those access rights.

Annex 15
Access Control Rules and Rights for Users

1. Scope

All users/user groups that need to access organizational information have specific, pre-determined access rights to information, operating systems and applications that conform to and are restricted by the Access Control Policy (Annex 18).

2. Responsibilities

2.1 The IT Director is responsible for creating, documenting and maintaining individual user/user group profiles that meet the requirements of the Access Control Policy (annex 18).

2.2 User access administration is carried out in line with Annex 14.

3. Procedure

3.1 *[This section should set out how you create user profiles, summarising (by operating systems and application) into standard profiles the individual user/user group access rights and the business requirements met by the controls, taking into account the Access Control Policy and ensuring that application level access control is consistent with the network level access control. This procedure should reference GDPR-C DOC 9.2.3, which deals with administration of user rights. This is also the place to deal with group IDs (ID = username). For preference, your rule should be that you do not allocate group IDs – if you have to, this is where you explain why. It might be because you have some functions where you do not need to track users and can safely provide read-only access. It might be because there is no other option, in which case you need to be clear about what other controls you might put in place. Access rights are: read, write, delete and execute, and these rights need to be allocated in respect of each system and application. You need to identify how you enforce access rights to applications in line with (ISO 27002 Clause 9.4.1) information classification levels and that application outputs are sent only to authorised users.]*

4. Classification of users

4.1 Users are also classified in terms of the level of access they need to information and systems. These classification levels, which are to be recorded in user agreements, are set out below:

Classification of data users		
Classification	**Access rights**	**Example**
Guest	Able to see and read public data. Full create and edit rights to a Private data space.	Clients
Trustee	Full rights to a shared directory or sub system. Able to see and use basic business templates and core information sources and systems.	Partner organizations Software maintenance Data input staff Anyone who has signed a non-disclosure agreement

Classification of data users		
Classification	**Access rights**	**Example**
Individual	Premises access – persons are permitted to gain physical access to premises, buildings or rooms where data processing systems are located. System access – access to data processing systems is permitted with prior authorization. Data access – persons are entitled to use data processing systems in order to gain access to the data to which they have a right of access for their work only. Personal data cannot be read, copied, modified or removed without prior authorization. Able to create files in a user group and delete owned files in that user group. Able to grant access rights to 'Private' files or directories to others. Access rights to restricted and confidential information dependent on role requirements.	xyz@ceu.edu
Supervisor	Full unrestricted rights to create new users and configure PCs and create user groups and manage the network.	IT staff
Administrator	Full unrestricted rights to defined systems and the ability to create and remove system supervisors.	IT Department [CEO] has right to read and edit all confidential/restricted documents

5. Privileges

5.1 Privileges are allocated in line with the requirements of Annex 14 – Subject Access Request Record.
The available privileges for each operating system, application and other system at CEU are: *[insert/attach a matrix or schedule that shows these, together with the level of user to which they could be allocated].*

6. User authentication

6.1 Users are authenticated at logon by providing both their username and their password within the parameters of the log-on system.
[This is where you should detail the other logon requirements that sit outside your single sign-on set up, and which might also refer to device authentication].

Annex 16
Notebook Computer Security

1. Scope[10]

All users of CEU's notebooks, computers and other mobile devices are within the scope of this procedure.

2. Responsibilities

2.1 The IT Director is responsible for specifying and/or providing the firewalls, anti-malware software, automatic updating, connectivity and backup facilities required under this procedure.
2.2 The IT Director is responsible for user training.
2.3 All users have specific responsibilities in terms of their User Agreements.

3. Procedure

3.1 CEU requires notebook computer level deployment of CEU firewalls, anti-malware software, and automatic updating facilities that are all up to date and meet the corporate minimum standards, which are specified in the User Agreement.
3.2 CEU requires notebook computer level deployment of the corporate policy on usernames and passwords, to have a password protected screensaver, and to encrypt all folders containing corporate information, and to disable folder and printer sharing, all of which is specified in the User Agreement.
3.3 CEU requires notebook computers that carry personal data, or are able to connect to systems that store or process *[personal data]*, use full-disk encryption. CEU's full-disk encryption solution is Bitlocker – built-in solution in Windows operating systems.
3.4 CEU requires that notebook computers are physically protected against theft and damage while in transit, in storage or in use and that, in cases of loss or theft, the specified corporate policy (see User Agreement) for dealing with such incidents is followed.
3.5 CEU requires users (in the User Agreement) to ensure that all the most recent operating system and application security-related patches, fixes and updates have been installed.
3.6 CEU requires (in the User Agreement) that notebook computers are backed up in line with corporate specification *[set out where?]*.
3.7 CEU requires users of notebook computers to carry with them at all times the chargers and spare batteries specified in the User Agreement.
3.8 CEU requires users to comply with the corporate requirements *[set out where?]* on the means of connecting to public access points, *[and accessing corporate information, both]* as described in the User Agreement.
3.9 CEU requires users, in the User Agreement, to act with care in public places so as to avoid the risk of screens and *[confidential]* notebook computer activity being overlooked by unauthorized persons.
3.10 CEU carries out regular and ad hoc audits of all notebook computers to ensure that they are configured in compliance with this procedure.
3.11 CEU provides users with appropriate training and awareness to ensure that they understand the risks of wireless on the road computing and that they understand and can carry out their agreed security obligations.

---

[10] **Chapter 21** of IT Governance: An International Guide to Data Security and ISO27001/ISO27002 deals with mobile computing. This template will need to be expanded to take into account mobile phones, Blackberries, PDAs and any other mobile devices, and adjusted to reflect different decisions on connectivity.

3.12 Work instruction *ISMS DOC [ ]* sets out how the corporate requirements set out in Clause 3.1 and 3.4 above are enforced.

3.13 *[WI ISMS DOC [ ]]* sets out how the *[VPN or other connectivity solution]* is to be operated.

3.14 *[WI ISMS DOC [ ]]* sets out how e-mails are to be encrypted when sent from mobile devices.

Annex 17
Complaints Procedure

1. Scope

This procedure addresses complaints from data subject(s) related to the processing of their personal data, CEU's handling of requests from data subjects, and appeals from data subjects on how complaints have been handled.

2. Responsibilities

2.1 Members of CEU Community are responsible for ensuring any complaints made in relation to the scope of this procedure are reported to the Data Protection Officer.
2.2 The Data Protection Officer is responsible for dealing with all complaints in line with this procedure.

3. Procedure

3.1 CEU has the contact details of its Data Protection Officer published on its website *[URL]*, clearly under the 'Contact us' section.
3.2 CEU has clear guidelines on this page *[URL]* and *[contact us form, which is sent directly to the Data Protection Officer's mailbox]*, that enable the data subject to lodge a complaint.
3.3 CEU clearly provides data subject(s) with the privacy notice (Annex 9 – Privacy Notice) by publishing it on its website *[URL/download link]*, clearly under the 'Contact us' section and relative to the complaints form submission.
3.4 Data subjects are able to complain to CEU about:
- 3.4.1 how their personal data has been processed
- 3.4.2 how their request for access to data has been handled
- 3.4.3 how their complaint has been handled
- 3.4.4 appeal against any decision made following a complaint.

3.5 Data subject(s) lodging a complaint with CEU's Data Protection Officer are able to do so by *[contact form published [at this location] on the company website, and/or via email direct to the Data Protection Officer as published [at this location] on the website]*.
- 3.5.1 Complaints received via the *[contact form]* are directed to the Data Protection Officer for resolution.
- 3.5.2 Complaints are to be resolved within *[timeframe]*.
- 3.5.3 Appeals on the handling of complaints are to be resolved within *[timeframe]*.

3.6 If CEU fails to act on a data subject's access request within one month, or refuses the request, it sets out in clear and plain language the reasons it took no action/refusal. CEU will also inform the data subject(s) of their right to complain directly to the supervisory authority. In doing so, CEU provides the data subject(s) with the contact details of the supervisory authority and informs them of their right to seek judicial remedy.

Annex 18
Access Control Policy

1 CEU controls access to information on the basis of 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 classification levels of information processed within that application and ensure that there is consistency between the classification levels and access control requirements across the systems and network(s).
f. Data protection (EU GDPR) and privacy, legislation and contractual commitments regarding access to data or services.
g. The 'need to know' principle (i.e. access is granted at the minimum level necessary for the role).
h. 'Everything is generally forbidden unless expressly permitted'.
i. Rules *[which ones]* that must always be enforced and those that are only guidelines *[how do you take this into account?].*
j. Prohibit *[how?]* user initiated changes to information classification labels (see Annex 24).
k. Prohibit *[how?]* user initiated changes to user permissions.
l. Enforcing *[how?]* rules that require specific permission before enactment.
m. Any privileges that users actually need to perform their roles, subject to it being on a need-to-use and event-by-event basis.

5 CEU has standard user access profiles for common roles in CEU (see Annex 15).

6 Management of access rights across the network(s) is *[done how?]*.

7 User access requests, authorization and administration are segregated as described in Annex 15.

8 User access requests are subject to formal authorization, to periodic review and to removal.

Annex 19
Individual User Agreement

1. Name:

Position:

Department:

Access rights: *[Insert the detailed access rights to be granted in terms of in* Annex 15 and levels of confidentiality the user is entitled to access.

User access request originated by: Respective Unit/Department
[Date]
User access request approved by: Manager/Executive (generic/line)
[Date]
User access request approved by: *[Asset owner(s)]*
[Date]
User acceptance of access rights and responsibilities as set out in this agreement:
Signed and agreed by staff member:
[Date]
User access name allocated:
E-mail address allocated:
Data storage file allocated:
User access request processed: IT Department
[Date]

1.1 I, *[ ],* accept that I have been granted the access rights defined in this agreement to those organizational information assets also identified in this agreement. I understand and accept the rights which have been granted, I understand the business reasons for these access rights, and I understand that breach of them, and specifically any attempt to access services or assets that I am not authorized to access – including any attempts to read, copy, modify or remove any personal data without prior authorization - may lead to disciplinary action and specific sanctions. I also accept and will abide by CEU's *[Internet Acceptable Use Policy, its e-mail policy and its information security weakness and event reporting policy]*. I understand that failure to comply with this agreement, or the commission of any information security breaches, may lead to the invocation of CEU's disciplinary policy.

1.2 I acknowledge that I have received adequate training in all aspects of my use of CEU's systems and of my responsibilities under this agreement.

2. Passwords

2.1 My username and password will be issued in line with CEU's procedure for authorising and issuing them.
2.2 I will change my initial temporary password at first logon.
2.3 I will select and use passwords that are at least 12 characters in length, are alpha-numeric, are not based on any easily guessable or memorable data such as names, dates of birth, telephone numbers etc., are not dictionary words and are free of consecutive identical all-numeric or all-alphabetic characters.
2.4 I will keep my password secret and will not under any conditions divulge it to or share it with anyone, nor will I write it down and leave it anywhere that it can easily be found

by someone else or record it anywhere without having obtained the specific authorization of the IT Director to do so.

2.5 I will not store my password in any automated logon process.

2.6 I will change my password at intervals as required by CEU, will not attempt to re-use passwords or use new passwords that are in a sequence, and will change my password more frequently if there is evidence of possible system or password compromise.

2.7 I will not use the same password for organizational and personal use.

2.8 Replacement passwords are administered as set out in Annex 14; users must obtain the written permission of the IT Director before a replacement password can be issued.

2.9 *[Insert any additional information regarding additional authentication requirements, e.g. biometrics, tokens, etc.]*

3. Clear desk policy, screen savers and information reproduction

3.1 I understand that I am required to ensure that no confidential or restricted information (in paper or removable storage media format) is left on my desk, in my environs, or left in or near reproduction equipment (photocopiers, fax machines, scanners) when I am not in attendance and will ensure that such information is secured in line with CEU's security requirements as set out in Annex 24.

3.2 I understand that I am required to ensure that no one is able to access my workstation when I am not in attendance and that I must have a password protected screensaver that operates within five minutes of no activity or which I activate when I leave the workstation unattended.

3.3 I know that I am required to terminate active computer sessions when I have finished them and to log off (i.e. not simply turn off the computer screen) whenever I am finished working *[and that the workstation is to be protected by appropriate key locks when I am away from the building]*.

3.4 I accept that I am not allowed to *[use/bring in to the office]* personal storage media, MP3 players, digital cameras and mobile phones with photographic capability.

3.5 I accept that I may only use CEU's reproductive equipment (photocopiers, fax machines, scanners) for proper organizational purposes and that I will ensure that I will use facilities that are appropriate for the classification level of any information with which I am dealing.

4. Software

4.1 I will ensure that no attempts are made to disable or over-ride any of CEU's installed software, including anti-malware software, firewalls and automatic updating services.

4.2 I accept that I may not download from the Internet or install on any organisational computer or other device any software of any sort for which CEU does not have a valid licence and that has not had the prior authorisation of the IT Director. I recognise that this prohibition includes freeware, shareware, screensavers, toolbars and/or any other programs that might be available.

5. Data control and legislation

5.1 I will obtain the written authorisation of the Data Protection Officer for the storage of any personal data (mine or anyone else's) on CEU's computer systems.

5.2 I will ensure that I abide by any legal requirements in respect of my computer use, including privacy and data protection regulations.

6. Backup and information classification

6.1 I acknowledge that I am responsible for ensuring that all information on my workstation is correctly classified and labelled in line with the requirements of Annex 24. I will ensure that this requirement is complied with.
6.2 I acknowledge that I am responsible for backing up information on my workstation.
6.3 I understand that I am required to store all data *on institutionally supported locations such as OneDrive, SharePoint or O:drive* and that I may not store information on the local drives of my computer.

7. Maintenance

7.1 I accept that I am responsible for the physical security of my workstation and will report any faults to IT helpdesk immediately.

8. Revocation and change of access rights

The access rights are only valid for the period of stay at CEU (active student status, active employment or assignment contract).

ANNEX TO THE USER AGREEMENT

This annex contains details of notebook configurations, service connection and backup procedures that may change from time to time.

Annex 20
Subject Access Request Record

1. DATA SUBJECT DETAILS:

Title	Mr ☐	Mrs ☐	Miss ☐	Ms ☐	Other: ☐
Surname					
First name(s)					
Current address					
Telephone number:					
Home					
Work					
Mobile					
Email address					
Date of birth					
Details of identification provided to confirm name of data subject:					
Details of data requested:					

1.1 DETAILS OF PERSON REQUESTING THE INFORMATION (if not the data subject):

Are you acting on behalf of the data subject with their *[written]* or other legal authority?	Yes ☐ No ☐
If 'Yes' please state your relationship with the data subject (e.g. parent, legal guardian or solicitor)	
Please enclose proof that you are legally authorized to obtain this information.	

Title	Mr ☐	Mrs ☐	Miss ☐	Ms ☐	Other: ☐
Surname					
First name(s)					
Current address					
Telephone number:					

Home	
Work	
Mobile	
Email address	

2. DECLARATION

I, ……, the undersigned and the person identified in (1) above, hereby request that Central European University provide me with the data about me identified above.

Signature: Date:

SAR form completed by (employee name):

I, ……, the undersigned and the person identified in (1.1) above, hereby request that Central European University provide me with the data about the data subject identified in (1) above.

Signature: Date:

SAR form completed by (employee name):

This form must immediately be forwarded to Central European University's Data Protection Officer.

Annex 21
Data Subject Consent Withdrawal Form

I, *[data subject name]*, withdraw my consent to process my personal data from Central European University/Közép-európai Egyetem/ CEU Educational-Service Non-profit Llc./ Central European University Foundation of Budapest (hereinafter "CEU"). CEU no longer has my consent to process my personal data for the purpose of *[specify legitimate reason of processing personal data]*, which was previously granted.

Signed by data subject:

Date:

Request actioned:

Data Protection Officer

Date:

Annex 22
Withdrawal of Consent Procedure

1. Scope

This procedure addresses the data subject(s) right to withdraw consent for the processing of his or her personal data.

Withdrawal of consent by the data subject means an unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies withdrawal of consent to the processing of personal data relating to him or her.

Withdrawal of consent shall be without effect to the lawfulness of processing based on consent before its withdrawal. Whereas consent covered all processing activities carried out for the same purpose or purposes, withdrawal of consent covers all processing activities carried out for the same purpose or purposes.

2. Responsibilities

As a data controller, CEU is responsible under the GDPR for administering withdrawal of consent from the data subject under advisement from Data Protection Officer.

3. Withdrawal of consent procedure

3.1 CEU demonstrates the data subject has withdrawn consent to the processing of his or her personal data as recorded in the (Annex 21 – Data Subject Consent Withdrawal form).

3.2 Where the processing had multiple purposes, CEU demonstrates withdrawal of consent for each purpose as recorded in the (Annex 21 – Data Subject Consent Withdrawal form).

3.3 The processing activities that relied upon the consent is stopped in accordance with the relevant process. The Data Protection Officer will inform the relevant process owner of this change so that processing can be stopped.

4. Withdrawal of parental consent procedure

4.1 CEU demonstrates the holder of parental responsibility over the specified child has withdrawn consent (Annex 25 – Parent Consent Withdrawal).

4.2 CEU demonstrates that reasonable efforts have been made to establish the authenticity of the parental responsibility by *[]*, when withdrawing consent for the specified child, considering available technology.

4.3 The processing activities that relied upon the consent is stopped in accordance with the relevant process. The Data Protection Officer will inform the relevant process owner of this change so that processing can be stopped.

Annex 23
Retention and Disposal Schedule

Template for retention and Disposal Schedule in a form of an excel file is available here: https://ceuedu.sharepoint.com/:x:/r/gdpr/Templates/ANNEX_23_%20GDPR_REC_4.9.xlsx?d=w4c1993e317e0446ea978a46e4dda7a10&csf=1&e=jwalwn

Annex 24
Information Security Classification Guidelines

1. Scope

All CEU's information assets and services, and personal data activities are classified, taking into account their legality, value, sensitivity and criticality to CEU.

2. Responsibilities

2.1 The owner of each asset is responsible for its classification, for ensuring it is correctly labelled and for its correct handling in line with its classification.
2.2 The intended recipient of any information assets sent from outside CEU becomes the owner of that asset.
2.3 The Chief Financial Officer (CFO) is responsible for maintaining the inventory of assets and services together with their classification levels.
2.4 The IT Director is responsible for the technical labelling mechanisms.
2.5 The IT Director is responsible for the creation, maintenance and review of electronic distribution lists and for ensuring that they conform to this security classification system.
2.6 All users of organisational information assets (including mobile phones, PDAs and other peripherals) have specific responsibilities identified in their user agreements.
2.7 The management of CEU is responsible for ensuring that *[mail/postal services, voicemail and voice, fax, photocopiers, couriers, etc.]* services and sensitive documents (including cheques, invoices, headed notepaper) are handled in line with the requirements of the GDPR.

3. Classification

3.1 CEU classifies information into four levels of classification: confidential, restricted, private and public.
3.2 The classification level of all assets is identified, both on the asset and in the information asset inventory.
3.3 The classification information must be included in the document footer, which must be manually set to appear on all pages of the document, or on the media on which it is recorded, in line with Clause 8, below.
3.4 Information received from outside CEU is reclassified by its recipient (who becomes its owner) so that, within CEU, it complies with this procedure.
3.5 Information that is not marked with a classification level is returned to its sender for classification; if it cannot be returned, it is destroyed.
3.6 The classifications of information assets are reviewed every *[six months]* by their owner and if the classification level can be reduced, it will be. The asset owner is responsible for declassifying information.
3.7 Confidential: this classification applies to information that is specifically restricted to the Board of Directors and specific professional advisers.
  3.7.1 Information that falls into this category must be marked 'Confidential', and its circulation is kept to a minimum *[with the names of the people to whom it is limited identified on the document]*. *[Each copy of a document that has this level of classification is numbered and a register is retained identifying the recipient of each numbered copy.]*
  3.7.2 Examples of confidential information might include information about potential acquisitions or corporate strategy, or about key organisational personnel, such as the Chief Executive Officer (CEO).

3.7.3 Confidential information sent by email must be encrypted and digitally signed and sent only to the e-mail box of the identified recipient.

3.7.4 Confidential information can only be sent by fax if the nominated recipient is available to receive it directly from the fax machine.

3.7.5 Confidential information can only be processed or stored on facilities that have been assessed as providing adequate security for such information. This classification is recorded on the information asset inventory and/or data inventory (DPIA Tool, Annex 3).

3.7.6 The amount of information that falls into this category should be carefully limited; the cost and operational inconvenience of protecting it properly is such that it needs only to be information whose release can significantly damage CEU.

3.8 Restricted: information of this category is restricted to Members of CEU Community above the level of:

3.8.1 Examples of restricted information include draft statutory accounts, which might be available to everyone in senior management, or implementation plans for corporate restructuring, which senior managers need to work through prior to their being rolled out.

3.8.2 Restricted information sent by email must be encrypted and digitally signed and sent only to the e-mail box of individuals known to be allowed to receive such information.

3.8.3 Restricted information can only be sent by fax if a recipient from the required level is available to receive it directly from the fax machine.

3.8.4 Restricted information can only be processed or stored on facilities which have been assessed as providing adequate security for such information. This classification is recorded on the information asset inventory and/or data inventory.

3.9 Private: this classification covers all information assets that have value but which do not need to fall within either of the other categories.

3.9.1 Everyone employed by CEU is entitled to access information with this classification.

3.9.2 This information has no restrictions in terms of how it is communicated, other than that it is not cleared for release outside CEU.

3.10 Public: this is information which can be released outside CEU.

4. Labelling

4.1 Documents are labelled as set out above, in the document footer. Documents that do not have footers are marked by addition of a physical, stick-on label.

4.2 Removable and storage media (CD-ROMs, USB sticks, tapes, etc.) are labelled *[describe any colour-coded systems used to indicate classification levels].*

4.3 Electronic documents and information assets are labelled by *[insert mechanism]*.

4.4 Information processing facilities are labelled *[describe how, if this clause is relevant]*. CEU.

5. Handling

5.1 Information assets can only be handled by individuals that have appropriate authorisations or on facilities that *[meet what requirements?]*.

5.2 The requirements for transmission, receipt, storage and declassification of classified and restricted information are described above. Destruction of information media can only be carried out by someone who has an appropriate level of authorisation.

5.3 CEU requires that confidential documents are only circulated *[in secure pdf format] / [as read-only documents]*.

5.4 Portable and storage media (including spooled media) must be moved, received and stored on the basis of the highest classification item recorded on them, and are subject to the physical security controls *[meet what requirements?]*, and are *[protected appropriately]* while being recorded.

5.5 For agreements with external organisations (Annex 26) which include information sharing, include a matrix for translating their security classifications into this one.

Annex 25
Parental Consent Withdrawal

I, *[parent/legal guardian name]*, would like to withdraw my consent to process *[child subject name]*'s personal data from Central European University / Közép-európai Egyetem/ CEU Educational-Service Non-profit Llc./ Central European University Foundation of Budapest (hereinafter as "CEU") *[and third party processor]*. CEU *[and third-party processor]* no longer has my consent to process the personal data of *[child subject name]* for the purpose of *[specify legitimate reason of processing personal data]*, which was previously granted.

I understand that the processing will be stopped as soon as possible, if not immediately, in an online automated environment. However, there may be a short delay while the withdrawal is processed.

The withdrawal of consent does not affect the lawfulness of the processing up to this point.

I am able to withdraw their consent to processing without suffering any detriment.

Signed by parent/guardian:

Date:

Request actioned:

Data Protection Officer

Date:

Annex 26
External Parties: Information Security Procedure

1. Scope

CEU maintains the security of its information processing facilities and information assets in relation to external parties. All external parties who need to access any organizational information assets are subject to this procedure.

CEU has (or may have) external party agreements with the following categories of organizations, all of whom are covered by this procedure; risks may be assessed for external parties as individual organizations or as categories, depending on the level of risk involved:

a. Service providers
b. Managed security services
c. Customers
d. Outsourcing suppliers (facilities, operations, IT systems, data collection, call centers, others)
e. Consultants and auditors
f. Developers and suppliers of IT systems and services
g. Cleaning, catering and other outsourced support services
h. Temporary personnel, placement and other (casual) short-term appointments

2. Responsibilities

2.1 Data Protection Officer is responsible for services in any of the above categories that include personal data, are required to ensure that external parties have entered into a formal external party agreement under this procedure, and that transitions (of information, information processing facilities, and any other information assets or personnel) are planned and executed without a reduction in the level of security that existed prior to commencement of the transition.

2.2 The Data Protection Officer is responsible for ensuring that the security controls, service definitions and delivery levels included in external party agreements are implemented, maintained and operated by the external party.

2.3 The IT Director is responsible for carrying out risk assessments where required by this procedure.

3. Procedure

Where there is a business need for working with external parties, CEU ensures that its information security is not reduced; access to University assets is not granted until a risk assessment has been completed, appropriate controls identified and implemented.

4. Risk Identification

4.1 CEU carries out a risk assessment to identify risks related to external party access and the possible need to complete a data protection impact assessment (Annex 10).

4.2 The risk assessment identifies and documents, for each external party:

a. The information processing facilities and information assets the external party will access.
b. The type of access the third party will have – physical access and/or logical access (identifying the assets that will be accessed), whether the access is taking place on site or off site and the exact location from which access will be made.

c. The value and classification (Annex 24) of the information that will be accessed.
d. The information assets that the external party are not intended to access and which may require additional controls to secure.
e. The external party's personnel, including their contractors and partners, who will or might be involved.
f. How external party personnel are to be authenticated.
g. How the external party will process, communicate and store information.
h. The impact to the external party of access not being available when required, or of inaccurate or misleading information being entered, received or shared.
i. How CEU's information security incident management procedure (Annex 27 and Annex 28) will be extended to incorporate information security incidents involving the external party.
j. Any legal, regulatory or other contractual issues that should be taken into account with respect to the external party.
k. How the interests of other stakeholders might be affected by any decisions.

5. Controls are selected in line with the requirements of the GDPR.

6. CEU implements those controls that are within its own power, and in line with the requirements of the GDPR.

7. CEU agrees with the external party those controls that the external party is required to implement and documents them in an agreement (drawn up by CEU's legal counsel) that the third party signs. The obligations on the external party include ensuring that all its personnel are aware of their obligations.

8. The agreements between CEU and external parties (whether suppliers or customers) are created by CEU's legal counsel, (who shall specifically include or provide *[documented]* reasons for excluding any of the items on the checklist below, and the requirement for which may have been identified through the risk assessment, from any such contract):
a. The Information Security Policy
b. The controls identified as required through the risk assessment process (see 4 above), which may include procedures and technical controls.
c. A clear definition and/or description of the product or service to be provided, and a description of information (including its classification – Annex 24) to be made available.
d. Requirements for user and administrator education, training and awareness (Annex 7)
e. Provisions for personnel transfer.
f. Description of responsibilities regarding software and hardware installation, maintenance and de-commissioning.
g. Clearly defined reporting process, reporting structure, reporting formats, escalation procedures and the requirement for the external party to adequately resource the compliance, monitoring and reporting activities.
h. A specified change management process.
i. Physical controls, including secure perimeters.
j. Controls against malware
k. Access control policy
l. Information security incident management (Annex 27 and Annex 28)
m. The target level for service and security, unacceptable service and security levels, definition of verifiable performance and security criteria, monitoring and reporting.

n. The right to monitor and audit performance (including of the third party's processes for change management, vulnerability identification and information security incident management), to revoke activities, and to use external auditors.
o. Service continuity requirements.
p. Liabilities on both sides, legal responsibilities and how legal responsibilities (including data protection and privacy) are to be met.
q. The protection of intellectual property rights (IPR), including copyright.
r. Controls over any allowed sub-contractors.
s. Conditions for termination / re-negotiation of agreements, including contingency plans.

9. Information transfer agreements

Additional controls must (subject to an individual risk assessment in relation to each proposed agreement) be considered where the contract is for the transfer of information or software:
a. Specific management responsibilities and procedures on each side for notifying transmission, dispatch and receipt and any specific controls associated with each action.
b. Procedures to ensure non-repudiation and to ensure traceability.
c. The required standards for packaging and means of transmission.
d. The agreed labeling system (see Annex 24).
e. Courier selection and identification methods
f. Escrow agreements.
g. How information security incidents (loss of or damage to an information asset in transit) will be managed.
h. Data protection, copyright, software licensing
i. Any technical standards that are required for recording or reading software or information.
j. Any other special controls, such as cryptography

10. Managing changes to third-party services

CEU may need to agree changes to external party contracts and agreements to take account of changes that it makes to, or as a result of:
a. the services it currently offers to its clients;
b. new applications and systems it has developed or acquired;
c. modifications, changes or updates to its own policies and procedures;
d. new or amended controls arising from new risk assessments or information security incidents.

The external party may need to request changes to the contract in order to implement:
a. Changes or improvements to their networks or other infrastructure.
b. New or improved technologies, new products or new releases of current products.
c. New development tools, methodologies and environments.
d. New physical locations or physical services.
e. New vendors or other suppliers of hardware, software or services.

Any changes that may be required are subject to a new risk assessment (taking into account the criticality of the business systems involved) and review of the selected controls (see Clauses 4.1 and 5 above).

New controls, or changes to existing controls are identified, authorized, agreed with the third party, and made the subject of an agreed variation *[insert here a reference to exactly how contract variations are handled]* to the existing contract.

The Data Protection Officer is responsible for ensuring that the revised controls are implemented and incorporated into the existing review and monitoring arrangements.

11. Informal outsourcing

There are extensive IT services that are available to members of CEU via the internet which CEU will have no formal agreement or contract in place with - examples include email services and cloud storage providers. Users of such services are required to accept the provider's set terms and conditions and CEU has no ability to negotiate as it would via the formal outsourcing procedure.

The use of such services for storing University information present a real risk to CEU as there is no way CEU can ensure the confidentiality, integrity and availability of the information without a formal agreement in place. The storage of personal data with such providers is likely to be a breach.

In light of these risks, wherever possible, University staff must only use services provided or endorsed by CEU for conducting University business. CEU recognizes, however, that there are occasions when it is unable to meet the legitimate requirements of its members and that in these circumstances it may be permissible to use services provided by other third parties.

.

University staff must not configure their University email account to automatically forward incoming mail to third party services with which CEU has no formal agreement.

Annex 27
Reporting Weaknesses, Events and Personal Data Breaches Procedure

1. Scope

All users (whether Members of CEU Community, contractors or temporary employees and third-party users) and owners of University information and personal data assets or systems are required to be aware of and to follow this procedure.

2. Responsibilities

2.1 Users and owners of organisational information and personal data assets are required to follow this procedure for reporting information security events, weaknesses and personal data breaches, and this is documented in User Agreements.
2.2 Information security events, weaknesses and personal data breaches are reported to the IT Director in line with this procedure.
2.3 The IT Director is responsible for managing information security events, weaknesses and personal data breach responses (see Annex 29 and Annex 30).
2.4 The DPO is responsible user training and awareness and for selecting those events which can be used to support training activities.

3. Information Security Breaches Procedure

3.1 Information security weaknesses and events are reported immediately after they are seen or experienced, on form in Annex 28 *[describe precisely the mechanism for doing this – where are the forms (intranet or elsewhere), how does a user get the forms, what exactly is the mechanism for transferring the form to the Information Security Manager.]*
3.2 Users are not allowed to continue working after identifying a possible information security weakness, event or personal data breach.
3.3 *[A duress alarm is fitted in the following locations and Employees/Staff and contractors have been trained in when and how to use it. The Information Security Manager handles all responses to duress alarm signals, and there is a standing work instruction that sets this out.]*
3.4 The Information Security Manager reports back, by email, with a copy to the user's Manager/Executive (generic/line), to describe how the event or breach was dealt with and closed out.
3.5 A copy of this e-mail is filed, together with the incident/weakness/event report, and any documentation arising from the event and the response to it that has been generated by following Annex 29.

4. Personal Data Breaches Procedure

4.1 In the case of a personal data breach, the Data Protection Officer / GDPR Owner determines whether it requires the relevant statutory notifications under the EU GDPR in accordance with GDPR Breach Notification Procedure, Annex 30.

Annex 28
Schedule of Information Security Event Reports

Number	Reported by	Date and time	Affected system/asset	Incident type	Severity	"Incident"	"Vulnerability"	"Event"	Closed out date and time

Annex 29
Responding to Information Security Reports

1. Scope

All reports of personal data security weaknesses, events or incidents relating to any of CEU's personal data assets *[and events that should have been reported but were not]* are within the scope of this procedure.
In addition, any weaknesses, events or incidents detected through *[summaries, or link to a document containing, details of all the monitoring and alert services that are used to detect information security events, together with details of who gathers this information and how it is consolidated/analyzed to identify events]* fall within the scope of this procedure.

2. Responsibilities

2.1 Users are required to report information security and personal data weaknesses, events or incidents to the IT Director as well as the DPO, as set out in Annex 27.
2.2 *[Owners]* of *[monitoring and alert services]* are responsible for reporting those events (or sequences of events) that fall within the scope of Annex 27.
2.3 The IT Director responsible for coordinating and managing the response to the any reported weakness, event or incident, including documentation of all emergency steps taken, evidence collection, and closing out the event.
2.4 *[All technical staff and Members of CEU Community, contractors or third parties, are required to support the IT Director in dealing with an event, weakness or incident.]*
2.5 The IT Director authorises access to live systems or data.
2.6 Asset owners carry out actual accesses to live systems or data in dealing with an incident.
2.7 The IT Director is responsible for the contingency planning components of the working instructions identified in 3.5 below.

3. Procedure

3.1 The IT Director logs (on Annex 28) all information security and personal data reports immediately upon receipt, allocating to each a unique number and uses this log to ensure that all reports are analyzed and closed out.
3.2 All information security and personal data events, weaknesses and incidents are, immediately upon receipt *[link back to the communication mechanism described in Annex 27]*, assessed and categorized (with reasons, on the face of Annex 31) by the Information Security Manager. Initially, there are four categories: events, weaknesses, incidents and unknowns.
'Events' are occurrences that, after analysis, have no *[or very minor]* importance for information security or personal data.
'Vulnerabilities' are weaknesses that, after analysis, clearly exist as significant weaknesses compromising information security or personal data.
'Incidents' are occurrences of events (series of events) that have a *[significant]* probability of compromising CEU's information security or personal data, i.e. when there is a likelihood of high risk to the data subject.
'Unknowns' are those reported events or weaknesses that, after initial analysis, are still not capable of allocation to one of the four categories.
3.3 The 'unknowns' are subject to further analysis to allocate them to one of the other three categories as soon as possible.

The prioritization for responses, when there are multiple event reports to deal with, is: incidents, unknowns, vulnerabilities, events.

When there are multiple event reports in each category, the IT Director prioritizes responses in the light of the criticality of the business systems and information assets (including personal data) at risk, the danger of further compromise to CEU's information security and personal data, the resources at his/her disposal, and any relevant time constraints (such as reporting requirements for personal data breaches).

3.4 Incidents involving high-value, business critical systems or personal data are immediately reported to the IT Director.

3.5 Specific work instructions set out the necessary containment and corrective action and standing contingency plans in respect of the following types of information security and personal data incident:

Breach Notification Procedure	Annex 30
Internal Breach Register	Annex 32
Breach Notification Authority Form	Annex 32
Systems failure and loss of service	[..]
Malware, including viruses	[..]
Denial of service	[..]
Errors resulting from poor data	[..]
Breaches of confidentiality	[..]
Breaches of information integrity	[..]
Misuse of information systems	[..]
Non-standard incidents	[..]

3.6 The Information Security Manager seeks additional input from qualified technical staff, as necessary and where he/she considers the standing instructions to be inadequate, to analyze and understand the incident and to identify appropriate actions to contain it and to implement contingency plans.

3.7 The IT Director invokes actions as set out in the standing work instructions plus additional activity that he/she considers necessary to contain and recover from the incident, and to implement contingency plans.

[Where necessary, the IT Director *coordinates activity with other organizations.]*

The IT Director confirms that the affected business systems have been restored and that the required controls are operational before authorizing a return to normal working.

3.8 Once the incident is contained, and the required corrective action is completed, the IT Director reports to the DPO with a summary of the incident, identifying the cause of the incident and analyzing its progress, trying to identify how CEU could have responded earlier or more effectively, or preventive action that might have been taken in advance of the information, the effectiveness of the containment and corrective actions and the contingency plans, and how the incident was closed out (see 3.9 below).

3.9 The IT Director is responsible for closing out the incident: this includes any reports to external authorities (see Annex 30 and Annex 33); initiating disciplinary action by referring the incident under CEU's Code of Ethics; planning and implementing preventative action to avoid any further recurrence; collecting and securing audit trails and forensic evidence (see Annex 34); initiating any action for compensation from software, service *[or outsource]* suppliers and communicating with those affected by or involved in the incident about returning to normal working and any other issues.

3.10 The IT Director prepares a monthly report to the Information Security Committee which identifies (from the Event Reporting Log, Annex 28) the number, type, category and severity of information security or personal data incidents during the preceding month, the cost of containment and recovery, and the total cost of the losses arising from each incident, and recommends (where appropriate) additional controls that might limit the frequency of information security and personal data incidents, improveCEU's ability to respond, and reduce the cost of response.

3.11 All the incident reports from the period since the last management review are taken into account at the next one, to ensure that CEU learns from the incidents.

Annex 30
Personal Data Breach Notification Procedure

1. Scope

3.1 This procedure applies in the event of a personal data breach under Article 33 of the GDPR – *Notification of a personal data breach to the supervisory authority* – and Article 34 – *Communication of a personal data breach to the data subject*.

3.2 The GDPR draws a distinction between a 'data controller' and a 'data processor' in order to recognise that not all organisations involved in the processing of personal data have the same degree of responsibility. Each organisation should establish whether it is data controller, or a data processor for the same data processing activity; or whether it is a joint controller.

2. Responsibility

2.1 All users (whether Members of 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 (reference Annex 7).

2.2 Members of CEU Community, contractors or temporary personnel are responsible for reporting any personal data breach to the Data Protection Officer.

3. Procedure – Breach notification data processor to data controller

3.1 CEU reports any personal data breach or security incident to the data controller without undue delay. These contact details are recorded in the Internal Breach Register (Annex 32). CEU provides the controller with all of the details of the breach.

3.2 The breach notification is made by email and/or phone call.

3.3 A confirmation of receipt of this information is made in writing incl. email.

4. Procedure – Breach notification data controller to supervisory authority

4.1 CEU determines if the supervisory authority need to be notified in the event of a breach.

4.2 CEU 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 conducting data protection impact assessment against the breach (Annex 3).

4.3 If a risk to data subject(s) is likely, CEU reports the personal data breach to the supervisory authority without undue delay, and not later than 72 hours.

4.4 If the data breach notification to the supervisory authority is not made within 72, CEU's DPO submits it electronically with a justification for the delay.

4.5 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.

4.6 The following information needs to be provided to the supervisory authority (Annex 32):

- 4.6.1 A description of the nature of the breach.
- 4.6.2 The categories of personal data affected.
- 4.6.3 Approximate number of data subjects affected.
- 4.6.4 Approximate number of personal data records affected.
- 4.6.5 Name and contact details of the Data Protection Officer.
- 4.6.6 Consequences of the breach that have already occurred and which are likely to occur.

4.6.7 Any measures taken to address the breach.
4.6.8 Any information relating to the data breach (may be submitted in phases).

4.7 The Data Protection Officer notifies the supervisory authority. Contact details for the supervisory authority are recorded in the Schedule of authorities and key suppliers (Annex 33).
4.8 In the event the supervisory authority assigns a specific contact in relation to a breach, these details are recorded in the Internal Breach Register (Annex 32).
4.9 The breach notification is made by email and/or phone call.
4.10 A confirmation of receipt of this information is made by email, phone call, etc.

5. Procedure – Breach notification data controller to data subject

5.1 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 using this form/in accordance with the Data Protection Officer's recommendations.
5.2 The notification to the data subject describes the breach in clear and plain language, in addition to information specified in clause 4.6 above.
5.3 CEU takes measures to render the personal data unusable to any person who is not authorised to access it using encryption.
5.4 The data controller takes subsequent measures to ensure that any risks to the rights and freedoms of the data subjects are no longer likely to occur by *[]*.
5.5 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 informs those affected in an equally effective manner.
5.6 If CEU has not notified the data subject(s), and the supervisory authority considers the likelihood of a data breach will result in high risk, CEU will communicate the data breach to the data subject by *[]*.
5.7 CEU documents any personal data breach(es), incorporating the facts relating to the personal data breach, its effects and the remedial action(s) taken.

Annex 31
Information Security Weaknesses and Events Checklist

REPORT TO THE DPO

[Describe here how you want the report to be made – in paper, by email, or what – remembering the potential issues around using a compromised system to report the compromise.]

TYPES OF INFORMATION SECURITY EVENTS

Loss of service, functionality, equipment or other facilities
System, software or hardware malfunctions, unscheduled shut downs, unexpected system errors or overloads
Human errors
Non-compliances with requirements of the ISMS (including uncontrolled system changes)
Breaches of physical security arrangements
Access violations
Note: this is not a conclusive list of information security events.

WARNING:

Do not investigate what appears to be an information security event.
Do not attempt to prove an information security weakness.
Do not continue working after observing an information security event or weakness.
Failure to report information security weaknesses or events, and failures to comply with the information security reporting procedure (Annex 27) will be treated as disciplinary offences.

Name of person making report:
Position/role/status:
Name and title of line manager:
Office/location
Date and time of report:

This report concerns:
System/information asset description:
[Identifying serial number/asset number/system name/other mark]

Weakness or event:
Date and time weakness or event observed:
Observed by whom (if not person making the report):
Description of weakness or event:

[Please provide as much detailed information as possible: what malfunctioned, what (sequence of) actions you were executing at the time, what messages came up on your screen, what precise things or strange behaviour occurred, what appeared to be the breach or other issue, what services, facilities or equipment ceased to be available, awareness of any

human errors or non-compliance with organizational policies, procedures or work instructions, or breaches of physical security.]

EVENT ASSESSMENT

Initial analysis:
Event Incident Vulnerability Unknown
Reasons for assessment:

Final analysis
Event Incident Vulnerability Unknown
Reasons for assessment:

Signed:

(Person making this report)

The box below is for use by the Data Protection Officer.

Annex 32
Internal Breach Register

Internal Breach Register templates in Excel format are available here:

https://ceuedu.sharepoint.com/:x:/r/gdpr/Templates/ANNEX_32_GDPR_REC_4.5.xlsx?d=w430775a43a594d5e85671a168055e341&csf=1&e=Dm7Jam

Annex 33
Contact With Authorities Work Instruction

1. Scope

The requirement for contacting authorities is set out below. CEU complies with requirements for contact with authorities under all relevant laws including the EU GDPR.

2. Responsibilities

Each body listed in clauses 3 and 4 below has a nominated owner who is responsible for managing the relationship with the body. This responsibility includes initiating and maintaining the relationship, and ensuring that the contact information in the schedule to which this work instruction relates (Annex 33) is current and complete.

3. CEU, the data controller or processor, has published the contact details of the Data Protection Officer *[where?]* and communicated them to the supervisory authority.

3.1 The following Data Protection Officer contact details are correct, and are published *[location]*, and communicated to the *[supervisory authority]*:

3.2 The relationship between CEU and the supervisory authority is owned by Data Protection Officer.

3.3 The IT Director and the Data Protection Officer have version controlled copies of this document with their personal copies of the business continuity and disaster recovery plan.

Annex 34
Collection of Evidence

1. Scope

All information gathered during the course of responding to an information security and personal data incident is potentially evidence to be used in a disciplinary, criminal or civil action. All such evidence is within the scope of this procedure.

2. Responsibilities

2.1 The IT Director is responsible for collection and retention of information in respect of information security and personal data incidents.
2.2 The Data Protection Officer is responsible for ensuring that the IT Personnel is trained to an adequate level in the techniques of evidence collection required CEU's jurisdiction.

3. Procedure

3.1 Where the likelihood of legal, civil or criminal action is established early in the incident response process, the police or lawyers are involved as early as possible and their guidance is sought and followed in respect of evidence collection and retention. If the event, or the possible action, spans organizational or geographic boundaries, specialist lawyers must be consulted to ensure that evidence can be collected and how it should be collected. External advisers or third parties are subject to non-disclosure agreements (NDA).
3.2 In all other cases, all originals of paper documents have, attached to them, a signed and dated statement describing precisely where, and under what conditions, it was found, who found it, who witnessed the event, together with a machine date-stamped photocopy of the document that indicates its original state.
3.3 Either the original computer media should be removed and retained securely or copies of information on hard drives, in memory or on removable computer media should be taken (with a log of all actions during the copying process) with a witness present.
3.4 Paper documents or magnetic media must be kept securely.
3.5 Incidents involving personal data needs to be reported to the supervisory authority (Internal Breach Reporting and Breach Notification Form, Annex 32).

Annex 35
Communication Procedure

1. Scope

All internal and external communications related to personal data, data breaches, GDPR compliance or any other topic related to data protection by CEU are within the scope of this procedure. Where relevant, CEU's policies, procedures and work instructions may determine the requirements for specific internal or external communications. Where this is the case, those documents supersede the procedure below.

2. Responsibilities

2.1 Data Protection Officer is responsible for identifying any necessary internal/external communications relating to GDPR compliance.
2.2 The DPO responsible for identifying when internal or external communication will be necessary.
2.3 The DPO responsible for identifying requirements for internal and external communications and scheduling any necessary regular internal communications relevant to the GDPR.
2.4 The DPO is responsible for determining requirements for external communications and approving external communications.

3. Internal communications

3.1 The DPO identifies the necessity for internal communication.
3.2 The DPO identifies the content of the communication the appropriate audience.
3.3 The DPO composes the communication as appropriate.

4. External communications

4.1 The DPO identifies the necessity for external communication and makes available his/her contact details to the data processor/data controller, as well as to data subjects and the supervisory authority under the GDPR.
4.2 The DPO identifies the content of the communication and the appropriate audience for the communication.
4.3 The DPO composes the communication as appropriate, in accordance with CEU's style guide for external communications.

Annex 36
Treating Personal Data in Research

1. Privacy by design and by default

1.1 In your research design, address the six security and privacy principles (Point 6 of the Data Protection Policy).

1.2 Conduct a data protection impact assessment to identify risks and formulate countermeasures (please refer to Annex 10 and Annex 3 of the Data Protection Policy)

1.3 Communicate the security and privacy measures for your research with all participants and data subjects.

2. Before research

2.1 Make sure your data subjects are well informed about the purpose of the research and their risks before they sign the informed consent form (Annex 8 – Privacy Procedure and Annex 9 – Privacy Notice).

2.2 Only generate and use data that are relevant for the purpose of your research.

2.3 Use a computer with an encrypted hard drive, encrypt your sensitive data, use safe and secure file storage and sharing.

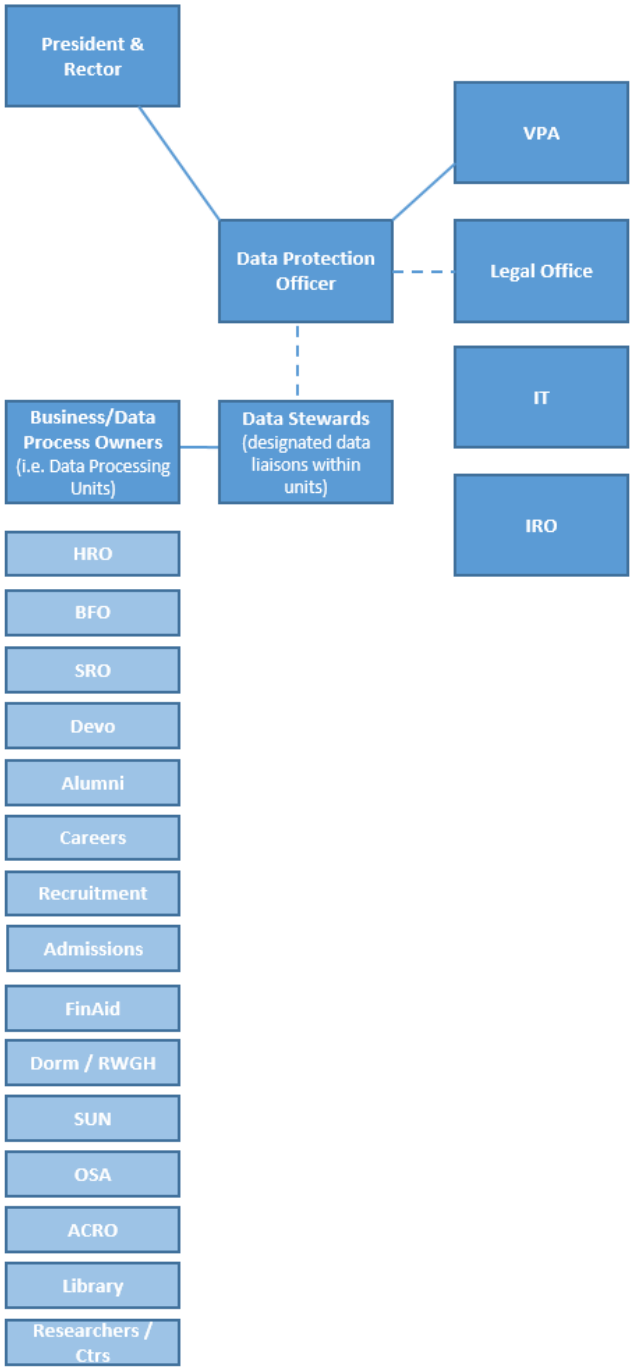
3. During research

3.1 Anonymize and/or pseudonymize the data and work with the de-identified data.

3.2 Work safe: do not leave printouts on the printer desk, do not use public wifi, do not work where others can easily watch your screen or can hear you talk.

3.3 During research feel free to consult the DPO in case of practical issues or just reflect on aspects.

Annex 37
Organizational Structure



Document information	
Type	Policy
Number	P-1805v1812
Title	Data Protection Policy
Distribution	Internal
Filename	P-1805v1812 Data Protection Policy
Notes	
Related documents	
For final documents	
Approved by:	Senate
Date of approval	May 9, 2018, modified on December 14, 2018.
Enters force	May 9, 2018