

<p>Personal Data Protection Policy of Közép-európai Egyetem and Central European University, New York</p>	<p>A Közép-európai Egyetem és a Central European University, New York személyes adatok védelméről szóló szabályzata</p>
--	--

**2017
Budapest**

Overview of the Personal Data Protection Policy of Közép-európai Egyetem, Budapest and Central European University, New York

The following overview provides a brief introduction to how personal data is handled at Közép-európai Egyetem, Budapest and Central European University, New York (collectively: the "University").

Data collected: the University controls personal data about its students, faculty and staff, and other individuals who come into contact with the University. The purpose of data controlling is to ensure the University to provide education and other associated functions in line with the applicable legal provisions.

Personal data: any information relating to the data subject (i.e. identified or identifiable *natural person*), in particular by reference to his/her name, an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity, and any reference drawn from such information pertaining to the data subject.¹

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

Consent: in cases where the University 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.

In all other cases (e.g. data management for the University's own purposes) the University requests the explicit consent of all data subjects

A Közép-európai Egyetem és a Central European University, New York személyes adatok védelméről szóló szabályzatának áttekintése

A jelen áttekintés röviden bemutatja a Közép-európai Egyetem és a Central European University, New York (együttesen az „Egyetem”) által történő személyes adatok kezelésének rendjét.

Személyes adatok gyűjtése: az Egyetem a hallgatóira, oktatóira és alkalmazottaira, valamint az Egyetemmel kapcsolatba kerülő egyéb személyekre vonatkozó személyes adatot kezel. Az adatkezelés célja az Egyetem oktatási tevékenységének, valamint egyéb, kapcsolódó feladatai ellátásának biztosítása a vonatkozó jogszabályok figyelembe vételével.

Személyes adat: az érintettel (azonosított vagy azonosítható *természetes személy*) kapcsolatba hozható adat – különösen az érintett neve, azonosító jele, valamint egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret -, valamint az adatból levonható, az érintettre vonatkozó következtetés.²

Jogszabályi követelmények: meghatározott esetekben, az Egyetem mint Magyarországon működő felsőoktatási intézmény, jogszabályi kötelezettségeinek teljesítése érdekében köteles meghatározott személyes adatokat gyűjteni, kezelni és továbbítani. Az Egyetem továbbá köteles a nemzeti hatóságok felszólításának eleget téve, meghatározott, a nemzeti hatóságok feladati ellátáshoz szükséges személyes adatokat továbbítani a hallgatókról, oktatókról és alkalmazottakról, illetve az Egyetemmel, annak működése során, kapcsolatba kerülő harmadik személyekről.

Hozzájárulás: azokban az esetekben, amikor az Egyetem jogszabályi előírás alapján köteles személyes adatot gyűjteni vagy továbbítani (beleértve a nemzeti hatóságok kérését is), az Egyetem az érintett személy hozzájárulását a személyes adatainak kezeléséhez nem szerzi be. Minden egyéb esetben (pl. az Egyetem saját céljait szolgáló adatkezelés) az Egyetem beszerzi valamennyi érintett személy kifejezett

¹ Point 2 of Article 3 of Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information.

² Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény, 3. § 2. pont

for the processing of their personal data before actual data processing takes place.

Personal Data Protection Policy: the detailed rules on how the University controls personal data can be found in the present Personal Data Protection Policy of the University (“Policy”). 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. It applies to all personal data managed by the University 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 the University community involved with 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.

Data protection in the course of scientific research: in the course of controlling data for scientific research, the University 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. Further aspects of controlling personal data by University researchers in the course of scientific research are determined in the University’s Ethical Research Policy.

Internal Data Protection Officer: the Rector of the University appoints an internal data protection officer to inspect the enforcement of the present Policy and, if needed, recommend its revision. The tasks of the internal data protection officer are described in Article 16 of the Policy; the name and availability of the internal data protection officer are indicated in Appendix 1.

hozzájárulását személyes adataik kezeléséhez, mielőtt az adatkezelésre sor kerülne.

Személyes adatok védelméről szóló szabályzat: az Egyetem által kezelt személyes adatokra vonatkozó részletes adatkezelési szabályokat a jelen Személyes adatok védelméről szóló szabályzat (a továbbiakban: „Szabályzat”) tartalmazza. A Szabályzat célja a személyes adatok pontos és biztonságos, valamint a vonatkozó nemzeti és Európai Uniói szabályoknak megfelelő kezelésének biztosítása. A Szabályzat hatálya valamennyi, az Egyetem által kezelt személyes adatra kiterjed, függetlenül az adat gyűjtésének, felhasználásának, rögzítésének, tárolásának, megsemmisítésének módjától, illetve függetlenül attól, hogy azok papír alapon vagy elektronikusan kerülnek tárolásra. Az Egyetem közösségének minden tagja, akik személyes adatot gyűjtenek, kezelnek vagy továbbítanak, köteles ismerni az adatkezeléssel összefüggő kötelezettségeit és felelősségét a jelen Szabályzat előírásainak maradéktalan betartásával.

Adatvédelem a tudományos kutatás során: a tudományos kutatás céljára történő adatkezelés során az Egyetem biztosítja az érintett jogát a személyes adatainak védelméhez a vonatkozó magyar és Európai Uniói adatvédelmi szabályoknak megfelelően, a jelen Szabályzatban meghatározottak szerint. Az Egyetem kutatói által a tudományos kutatásaik során alkalmazott személyes adatok kezeléséről az Egyetem Etikai Kutatási Szabályzata további szempontokat tartalmaz.

Belső adatvédelmi felelős: a jelen Szabályzat érvényesülésének ellenőrzésére és esetleges felülvizsgálatának kezdeményezésére az Egyetem rektora belső adatvédelmi felelőst nevez ki. A belső adatvédelmi felelős feladatait a jelen Szabályzat 16. §-a, mindenkor személyét és elérhetőségét a jelen szabályzat 1. számú melléklete tartalmazza.

* * * * *

**Personal Data Protection Policy
of
Közép-európai Egyetem
and
Central European University, New York**

**A Közép-európai Egyetem
és a
Central European University, New York
személyes adatok védelméről szóló
szabályzata**

PREAMBLE

With the Közép-európai Egyetem and the Central European University, New York (collectively: the “University”) being data controllers, the Senate of the University determines the University’s data controlling and data transfer procedure in compliance with the provisions on data processing in Articles 18 (2) and 19 of Act CCIV of 2011 on National Higher Education (“National Higher Education Act” or “NHEA”), Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information (“Data Protection Act” or “DPA”), Act CXIX of 1995 on the Use of name and Address Information Serving the Purposes of Research and Direct Marketing (“Research Data Control Act”), and Act V of 2013 on the Civil Code (the “Hungarian Civil Code”) as follows.

PART ONE

General Provisions

Article 1

Purpose of the Policy

The purpose of this Policy is to define the University’s procedures of keeping registers, comply with relevant legislation and abide by the requirements of data protection and data security. The right to informational privacy of the University’s students, faculty, employees and persons working under other legal relationship, as for instance agency

BEVEZETÉS

A Közép-európai Egyetem és a Central European University, New York (együttesen az „Egyetem”) mint adatkezelők tekintetében, az Egyetem szenátusa az Egyetemen folyó adatkezelést és az adatok továbbításának rendjét a nemzeti felsőoktatásról szóló 2011. évi CCIV. törvény (a továbbiakban: „Nftv.”) 18. § (2) és 19. §-ában meghatározott adatkezelés előírásainak való megfelelés érdekében, az adatvédelemmel kapcsolatos hatályos jogszabályokkal, így különösen az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: „Info. tv.”), a kutatás és a közvetlen üzletszerzés célját szolgáló név- és lakcímadatok kezeléséről szóló 1995. évi CXIX. törvény (a továbbiakban: „Kutatási Adatkezelési tv.”) és a Polgári Törvénykönyvről szóló 2013. évi V. törvény (a továbbiakban: ”Ptk.”) rendelkezéseivel összhangban az alábbiakban határozza meg.

ELSŐ RÉSZ

Általános rendelkezések

1. §

A jelen Szabályzat célja

A jelen Szabályzat célja az, hogy – az Egyetem hallgatói, továbbá oktatói, alkalmazottai, munkavállalói, valamint munkavégzésre vonatkozó egyéb jogviszony alapján, így például a megbízási jogviszony keretében munkát végző jogalanyok (a továbbiakban összefoglalóan: alkalmazott) - információs önrendelkezési jogának

relationship (hereinafter collectively: employees), shall always be honored.

tiszteletben tartása mellett – meghatározza az Egyetem nyilvántartásai vezetésének rendjét, továbbá biztosítja a jogszabályi rendelkezéseknek való megfelelést, az adatvédelem és adatbiztonság követelményeinek betartását.

Article 2

2. §

Scope of the Policy

A Szabályzat hatálya

The Policy applies to all registers of personal data kept by the University or its organizational units. Persons who under this Policy are responsible for data processing (the data processing officials) shall act in compliance with the Policy when handling the registers.

A Szabályzat hatálya kiterjed az Egyetemen vagy az Egyetem egyes szervezeti egységeinél vezetett valamennyi, személyes adatot tartalmazó nyilvántartásra. A jelen Szabályzat értelmében adatkezelésért felelős személynek minősülő személyek a nyilvántartások kezelése során a jelen Szabályzatnak megfelelően kötelesek eljárni.

Article 3

3. §

Definitions

Értelmező rendelkezések

1. *data subject* shall mean a natural person who has been identified by reference to specific personal data, or who can be identified, directly or indirectly;

1. *érintett*: bármely meghatározott, személyes adat alapján azonosított vagy – közvetlenül vagy közvetve – azonosítható természetes személy;

2. *personal data* shall mean any information relating to the data subject- in particular by reference to his name, an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity -, and any reference drawn from such information pertaining to the data subject;

2. *személyes adat*: az érintettel kapcsolatba hozható adat – különösen az érintett neve, azonosító jele, valamint egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret -, valamint az adatból levonható, az érintettre vonatkozó következtetés;

3. *special data* shall mean any personal data
a) revealing racial origin or nationality, political opinion and any affiliation with political parties, religious or philosophical belief or trade union membership and personal data concerning sex life,

3. *különleges adat*:
a) a faji eredetre, a nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdek-képviseleti szervezeti tagságra, a szexuális életre vonatkozó személyes adat,

b) concerning health, pathological addictions, or criminal record;

b) az egészségi állapotra, a kóros szenvedélyre vonatkozó személyes adat, valamint a bűnügyi személyes adat;

4. *personal data processed in criminal matters* shall mean personal data that might be related to the data subject or that pertain to any prior criminal offense committed by the data subject and that is obtained by organizations authorized to conduct criminal proceedings or investigations or by penal institutions during or prior to criminal proceedings in connection with a crime or criminal proceedings;

5. *consent* shall mean any freely and expressly given, specific and informed indication of the wish of the data subject by which the data subject signifies his/her unequivocal agreement to the processing, either wholly or partially, of personal data relating to him/her;

6. *objection* shall mean the statement of the data subject by which he/she objects to the processing of his/her personal data and requests termination of the data processing and/or deletion of the processed data;

7. *data controller* shall mean any natural or legal person or any organization without legal personality that individually or jointly with others determines the purpose of the processing of data, makes decisions on data processing (including those as to the means of the processing) and implements these decisions or has them implemented by the technical data processor he/she has commissioned;

8. *data control* shall mean any operation or set of operations which is performed upon data, irrespective of the applied procedure, such as collection, obtaining, recording, organization, storage, alteration, use, retrieval, transfer, making public, alignment or combination, blocking, deletion or destruction, as well as the barring of their further use, photographing, sound or image recording, as well as the recording of physical characteristics suitable for personal identification (such as fingerprints, and palmprints, DNA samples and iris images);

4. *bűnügyi személyes adat*: a büntetőeljárás során vagy azt megelőzően a bűncselekménnyel vagy a büntetőeljárással összefüggésben, a büntetőeljárás lefolytatására, illetve a bűncselekmények felderítésére jogosult szerveknél, továbbá a büntetés-végrehajtás szervezeténél keletkezett, az érintettel kapcsolatba hozható, valamint a büntetett előéletre vonatkozó személyes adat;

5. *hozzájárulás*: az érintett akaratának önkéntes és határozott kinyilvánítása, amely megfelelő tájékoztatáson alapul, és amellyel félreérthetetlen beleegyezését adja a rá vonatkozó személyes adatok - teljes körű vagy egyes műveletekre kiterjedő - kezeléséhez;

6. *tiltakozás*: az érintett nyilatkozata, amellyel személyes adatainak kezelését kifogásolja, és az adatkezelés megszüntetését, illetve a kezelt adat törlését kéri;

7. *adatkezelő*: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely önállóan vagy másokkal együtt az adatok kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajtatja;

8. *adatkezelés*: az alkalmazott eljárástól függetlenül az adaton végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adat további felhasználásának megakadályozása, fénykép, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy

	tenyéryomat, DNS-minta, íriszkép) rögzítése;
9. <i>data transfer</i> shall mean making data accessible for a specific third party;	9. <i>adattovábbítás</i> : az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele;
10. <i>public disclosure</i> shall mean making data accessible to the general public;	10. <i>nyilvánosságra hozatal</i> : az adat bárki számára történő hozzáférhetővé tétele;
11. <i>deletion of data</i> shall mean the destruction or elimination of data sufficient to make them irretrievable;	11. <i>adattörlés</i> : az adat felismerhetetlenné tétele oly módon, hogy a helyreállítása többé nem lehetséges;
12. <i>referencing</i> shall mean the marking of stored data for the purpose of identification;	12. <i>adatmegjelölés</i> : az adat azonosító jelzéssel ellátása annak megkülönböztetése céljából;
13. <i>blocking of data</i> shall mean the marking of stored data with the aim of limiting their processing in future permanently or for a predetermined period;	13. <i>adatzárolás</i> : az adat azonosító jelzéssel ellátása további kezelésének végleges vagy meghatározott időre történő korlátozása céljából;
14. <i>destruction of data</i> shall mean the complete physical destruction of the data carrier containing personal data;	14. <i>adatmegsemmisítés</i> : az adatot tartalmazó adathordozó teljes fizikai megsemmisítése;
15. <i>data processing</i> shall mean the technical operations involved in data control, irrespective of the method and instruments employed for such operations and the venue where it takes place, provided that such technical operations are carried out on the data;	15. <i>adatfeldolgozás</i> : az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől, feltéve hogy a technikai feladatot az adaton végzik;
16. <i>data processor</i> shall mean any natural or legal person or unincorporated organization that is engaged under contract in the processing of personal data, including when the contract is concluded by virtue of law;	16. <i>adatfeldolgozó</i> : az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely szerződés alapján - beleértve a jogszabály rendelkezése alapján kötött szerződést is - adatok feldolgozását végzi;
17. <i>data file</i> shall mean the totality of data contained in a filing system;	17. <i>adatállomány</i> : az egy nyilvántartásban kezelt adatok összessége;
18. <i>third person</i> shall mean any natural or legal person or unincorporated organization, other than the data subject, the controller or the processor;	18. <i>harmadik személy</i> : olyan természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely nem azonos az érintettel, az adatkezelővel vagy az adatfeldolgozóval;

19. *EEA Member State* shall mean any Member State of the European Union and any State that is a party to the Agreement on the European Economic Area, furthermore, any other country whose citizens are enjoying the same treatment as nationals of States who are parties to the Agreement on the European Economic Area by virtue of an agreement between the European Union and its Member States and a State that is not a party to the Agreement on the European Economic Area;
19. *EGT-állam*: az Európai Unió tagállama és az Európai Gazdasági Térségről szóló megállapodásban részes más állam, továbbá az az állam, amelynek állampolgára az Európai Unió és tagállamai, valamint az Európai Gazdasági Térségről szóló megállapodásban nem részes állam között létrejött nemzetközi szerződés alapján az Európai Gazdasági Térségről szóló megállapodásban részes állam állampolgárával azonos jogállást élvez;
20. *third country* shall mean any State other than EEA Member States;
20. *harmadik ország*: minden olyan állam, amely nem EGT-állam;
21. *personal data breach or privacy incident* shall mean the unlawful control or processing of personal data meaning, in particular, unauthorized access, alteration, transfer, disclosure by transmission, deletion, or destruction as well as accidental damage and destruction;
21. *adatvédelmi incidens*: személyes adat jogellenes kezelése vagy feldolgozása, így különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés;
22. *purpose-bound nature of data processing*: personal data shall be processed only for a specified purpose, in order to exercise a right or perform an obligation. This purpose shall be complied with in all phases of the data processing, recording of personal data shall be done under the principle of lawfulness and fairness. No personal data shall be processed unless indispensable and suitable for the achievement of the purpose of the data processing, and only to the extent and for the duration necessary to achieve that purpose.
22. *adatkezelés célhoz kötöttsége*: Személyes adatot kezelni csak meghatározott célból, jog gyakorlása és kötelezettség teljesítése érdekében lehet. Az adatkezelésnek minden szakaszában meg kell felelnie e célnak, az adatok felvételének és kezelésének tisztességesnek és törvényesnek kell lennie. Csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen, a cél elérésére alkalmas, csak a cél megvalósulásához szükséges mértékben és ideig.
23. *storage of personal data*: for the purpose of this Policy, the following activities shall mainly but not exclusively qualify as storage of personal data: storing personal and study data (collectively: storing student data), storing dormitory data, welfare data, data about fees and benefits, storing data about employees.
23. *nyilvántartás*: a jelen Szabályzat szempontjából nyilvántartásnak minősül különösen, de nem kizárólagosan a személyes és tanulmányi nyilvántartás (együttesen: hallgatói nyilvántartás), a kollégiumi nyilvántartás, a szociális, térítési és juttatási nyilvántartás, munkavállalói (alkalmazotti) nyilvántartás.
24. *scientific research*: an activity with the objective to increase knowledge of the world, its meaning and of the correlation of its
24. *tudományos kutatás*: az a tevékenység, amelynek célja a világról, annak jelentéseiről, a jelenségek összefüggéseiről

manifestations, for which name and address information or direct contact with private individuals is necessary in order to explore the objective correlation of the surveyed social, economic and natural circumstances.

25. *scientific researcher*: the natural person with a degree or title in science, being involved in scientific activities in his particular field or branch of science; as well as the person involved in scientific research according to a certificate received from an organisation pursuing scientific projects or from a foundation sponsor.

szerzett ismeretek gyarapítása, és amelynél a vizsgált társadalmi, gazdasági és természeti jelenségek objektív összefüggéseinek a feltárásához név- és lakcímadat vagy a személyekkel történő közvetlen kapcsolatfelvétel szükséges.

25. *tudományos kutató*: az a természetes személy, aki tudományos fokozattal, illetőleg címmel rendelkezik és abban a tudományágban vagy tudományterületen, amelyben felkészültségét bizonyította, tudományos tevékenységet végez; továbbá, aki kutatási feladatot is ellátó szervtől vagy alapítványi támogatótól kapott igazolás szerint tudományos kutatást végez.

PART TWO

The Rules of Data Control

Article 4

Purpose of Data Control

The University keeps registers to ensure that it could have access – inasmuch as the relevant laws approve that – to the data it needs for its proper operation, for the exercise of its employer’s rights and organize training activities. Those data may be processed to decide entitlement to, and the certification of, benefits ensured by law and the University’s Organizational and Operational Rules (“OOR”) that make it possible to establish the beneficiary’s identity and entitlement to a benefit.

The University may control data of its students, faculty and staff as well as third parties – in compliance with a relevant laws – only in connection with employment, the awarding of benefits and allowances and the imposition of obligations, the fulfillment of citizen’s rights and duties, for scientific research purposes, on grounds of national

MÁSODIK RÉSZ

Az adatkezelés szabályai

4. §

Az adatkezelés célja

Az Egyetem nyilvántartásai vezetésének célja az, hogy az Egyetem rendeltetésszerű működéséhez, az Egyetem mint munkáltató jogainak gyakorlásához és a képzés megszervezéséhez szükséges adatok – a vonatkozó jogszabályok által meghatározott körben – az Egyetem rendelkezésére álljanak. A jogszabályokban, valamint az Egyetem Szervezeti és Működési Szabályzatában („SZMSZ”) biztosított kedvezményekre való igényjogosultság elbírálásához és igazolásához szükséges célből azok az adatok kezelhetők, amelyekből megállapítható a jogosult személye és a kedvezményre való jogosultsága.

Az Egyetem a hallgatók, oktatók és alkalmazottak, valamint harmadik személyek személyes adatait – külön jogszabályban meghatározottak szerint - csak a foglalkoztatással, juttatások, kedvezmények, kötelezettségek megállapításával és teljesítésével, állampolgári jogok és kötelezettségek

security, and in order to process registers as defined by the NHEA – to the extent and for the duration necessary to achieve its purpose and bound by the purpose concerned, where it is necessary for the implementation of certain rights or obligations.

Article 5

Duration of Data Control

(1) In compliance with Article 18 (1) of the NHEA, the University shall register the following personal and special data essentially required to ensure

- a) the proper functioning of the institution,
- b) applicants' and students' rights and the fulfilment of their obligations,
- c) the organization of education and research activities,
- d) exercising employer rights, as well as those of lecturers, researchers and employees and to fulfil obligations,
- e) registering data as specified in relevant legislation,
- f) the determination, assessing and certifying allowance entitlements specified in legal regulations or in the organisation and operational manual of higher education institutions,
- g) the path tracking of graduates defined in Article 15 and 16 of the NHEA.

(2) The University may control

- a) the personal data of students in line with Subsection 3 of Section I/B of Annex 3 of the NHEA, only for a maximum of eighty years after the announcement of the termination of their student status;
- b) the data of employees (except point c) and d) below) – unless otherwise provided by social security legislation – in line with Subsection 3 of Section I/A of Annex 3 of the

teljesítésével kapcsolatosan, tudományos kutatás céljára, nemzetbiztonsági okokból, valamint az Nftv-ben meghatározott nyilvántartások kezelése céljából, a cél megvalósulásához szükséges mértékben és ideig, célhoz kötötten, jog gyakorlása és kötelezettség teljesítése érdekében kezelheti.

5. §

Az adatkezelés időtartama

(1) Az Nftv. 18. § (1) bekezdésével összhangban az Egyetem

- a) az intézmény rendeltetésszerű működéséhez,
- b) a jelentkezők és a hallgatók jogainak gyakorlásához és kötelezettségeinek teljesítéséhez,
- c) a képzés, kutatás megszervezéséhez,
- d) a munkáltatói jogok gyakorlásához, illetve az oktatók, kutatók, dolgozók jogainak gyakorlásához és kötelezettségeik teljesítéséhez,
- e) a jogszabályokban meghatározott nyilvántartások vezetéséhez,
- f) a jogszabályokban és a felsőoktatási intézmény szervezeti és működési szabályzatában biztosított kedvezményekre való jogosultság megállapításához, elbírálásához és igazolásához,
- g) az Nftv. 15. és 16. § szerint végzetek pályakövetése céljából nélkülözhetetlenül szükséges személyes és különleges adatokat tartja nyilván.

(2) Az Egyetem

- a) a hallgatók adatait az Nftv. 3. sz. melléklet I/B pont 3. alpontja alapján a hallgatói jogviszony megszűnésére vonatkozó bejelentéstől számított legfeljebb 80 évig;
- b) az alkalmazottak adatait (kivéve a lenti c) és d) pontot) – ha a társadalombiztosítási jogszabályok másként nem rendelkeznek – az Nftv. 3. sz. melléklet I/A pont 3. alpontja

NHEA, only for a maximum of five years after the termination of their employment;

c) the personal data of employees contained in the official certificate issued by the crime registration authority which are managed by the University for the purpose of confirming clean criminal records and that the employee has not been banned from his/her profession, until the date of the decision related to employing the employee, or - in the case of employment - until the end of the sixth month following the termination of the employment;

d) the personal data related to the faculty employed based on an assignment contract received based on the relevant provision of the NHEA – for the purpose of establishing the lack of existence of grounds for refusal –

(i) until the date of the decision made on the establishment on an assignment relationship,

(ii) in case of establishing and maintaining an assignment relationship, until the end of the assignment agreement.

(3) Following the expiry of the period defined by paragraph (2) above, the University shall arrange the destruction of said personal data.

(4) Personal data shall be deleted if

a) their processing is unlawful;

b) in the case of a voluntary supply of data, the data subject so requires;

c) the purpose of data processing ceases to exist or the deadline set by law of the further storage of the data concerned has expired;

d) a decision to that effect has been made by a court or by the National Authority for Data Protection and Freedom of Information (hereinafter the “Authority”);

e) they are incomplete or erroneous – and there is no legitimate way to rectify that – provided no rule of law prohibits deletion.

alapján a foglalkoztatás megszűnésétől számított legfeljebb 5 évig;

c) az alkalmazottak azon személyes adatait, amelyeket a bűnügyi nyilvántartó szerv által kiállított hatósági bizonyítvány tartalmaz, és amelyek a büntetlen előéletre és a foglalkozástól eltiltás hiányára vonatkozó feltétel ellenőrzése céljából kezel, az alkalmazás létesítésével összefüggésben meghozott döntés időpontjáig vagy - alkalmazás esetén - annak megszűnését vagy megszüntetését követő hatodik hónap végéig;

d) a megbízási jogviszony keretében foglalkoztatott oktatóra vonatkozó, az Nftv. vonatkozó rendelkezése alapján megismert személyes adatokat – a kizáró ok fennállásának megállapítása céljából –

(i) a megbízási jogviszony létesítéséről meghozott döntés időpontjáig,

(ii) a megbízási jogviszony létesítése és fennállása esetén a megbízási jogviszony megszűnéséig kezeli.

(3) A (2) szakaszban meghatározott időtartam elteltét követően az Egyetem gondoskodik a személyes adatok megsemmisítéséről.

(4) A személyes adatot törölni kell, ha

a) a kezelése jogellenes;

b) önkéntes adatszolgáltatás esetén az érintett azt kéri;

c) az adatkezelés célja megszűnt, vagy az adatok tárolásának törvényben meghatározott határideje lejárt;

d) azt a bíróság vagy a Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: „Hatóság”) elrendelte;

e) az hiányos vagy téves - és ez az állapot jogszerűen nem korrigálható -, feltéve, hogy a törlést törvény nem zárja ki.

Article 6

Officials Responsible for Data Control

(1) The Rector of the University, or some other person authorized by him, may appoint

6. §

Adatkezelésért felelős személyek

(1) Az Egyetem rektora vagy az általa meghatalmazott más személy az egyes

or designate officials responsible for data control in charge of keeping various registers. Appendix 1 attached to this Policy lists positions where the persons filling them qualify as persons responsible for data control without special appointment or authorization. Pursuant to Article 16 of the present Policy below, the Internal Data Protection Officer is authorized to inspect the activities of each of the persons responsible for data control within University.

(2) Signing a declaration of non-disclosure shall be a precondition for the appointment of a person responsible for data control. The relevant provisions on the consequences of violating the rules of personal data control are summarized in Appendix 4.

(3) The Internal Data Protection Officer shall regularly provide training for the persons responsible for data control about data protection.

Article 7

Data that may be Processed

(1) Personal data may only be processed,

- a) if the data subject has given his/her consent or
- b) when processing is necessary as decreed by law or by a local authority based on authorization conferred by law concerning specific data defined therein for the performance of a task carried out in the public interest (hereinafter referred to as “mandatory processing”).

(2) Personal data may be processed also if obtaining the data subject’s consent is impossible or it would give rise to disproportionate costs, and the processing of personal data is necessary

- a) for compliance with a legal obligation pertaining to the University, or

nyilvántartások vezetésére adatkezelésért felelős személyeket nevezhet, illetve jelölhet ki. A jelen szabályzat 1. sz. melléklete tartalmazza azokat a munkaköröket, amelyek betöltője külön kinevezés, illetve megbízás nélkül is adatkezelésért felelős személynek minősül. A belső adatvédelmi felelős jogosult minden, az egyetemi nyilvánvalóságok vezetésére kijelölt adatkezelésért felelős személy tevékenységének ellenőrzésére a jelen Szabályzat 16. §-ában foglaltak szerint.

(2) Adatkezelésért felelős személyként csak olyan személy nevezhető ki, aki titoktartási nyilatkozatot tesz. Az adatkezelési szabályok megsértésének jogkövetkezményeire vonatkozó jogszabályi rendelkezések összefoglalóját a 4. sz. melléklet tartalmazza.

(3) Az adatkezelésért felelős személyek részére az adatvédelmi ismeretek rendszeres oktatásáról a belső adatvédelmi felelős gondoskodik.

7.§

Kezelhető adatok

(1) Személyes adat csak abban az esetben kezelhető,

- a) ha ahhoz az érintetthozzájárult, vagy
- b) azt törvény vagy - törvény felhatalmazása alapján, az abban meghatározott körben– helyi önkormányzat rendelete közérdeken alapuló célból elrendeli (a továbbiakban: „kötelező adatkezelés”).

(2) Személyes adat kezelhető akkor is, ha az érintett hozzájárulásának beszerzése lehetetlen vagy aránytalan költséggel járna, és a személyes adat kezelése

- a) az Egyetemre vonatkozó jogi kötelezettség teljesítése céljából szükséges, vagy

b) for the purposes of the legitimate interests pursued by the University or by a third party, and enforcing these interests is considered proportionate to the limitation of the right for the protection of personal data.

(3) Where personal data is recorded under the data subject's consent, the University shall - unless otherwise provided for by law - be able to process the data recorded where this is necessary:

- a) for compliance with a legal obligation pertaining to the controller, or
- b) for the purposes of legitimate interests pursued by the University or by a third party, if enforcing these interests is considered proportionate to the limitation of the right for the protection of personal data, without the data subject's further consent, or after the data subject having withdrawn his consent.

(4) Before processing operations are carried out, the data subject shall be clearly and elaborately informed about all aspects concerning the processing of his/her personal data, such as the purpose for which his/her data is required and the legal basis, the person entitled to control the data and to carry out the processing, the duration of the proposed processing operation, and the persons to whom his/her data may be disclosed and whether information reporting is mandatory or voluntary. Information to be given to the data subject shall include his/her rights related to data control and his/her options for seeking legal remedy. In the case of mandatory data recording such information may be supplied by way of publishing reference to the legislation containing the information referred to in this paragraph. Appendix 2 attached to this Policy carries the data that the University is obliged to obtain pursuant to the NHEA.

(5) If the provision of information to the data subject proves impossible or would involve disproportionate efforts – especially in case of data processing for statistical or scholarly purposes -, the obligation of information may

b) az Egyetem vagy harmadik személy jogos érdekének érvényesítése céljából szükséges, és ezen érdek érvényesítése a személyes adatok védelméhez fűződő jog korlátozásával arányban áll.

(3) Ha a személyes adat felvételére az érintett hozzájárulásával került sor, az Egyetem a felvett adatokat törvény eltérő rendelkezésének hiányában

- a) a rá vonatkozó jogi kötelezettség teljesítése céljából, vagy
- b) az Egyetem vagy harmadik személy jogos érdekének érvényesítése céljából, ha ezen érdek érvényesítése a személyes adatok védelméhez fűződő jog korlátozásával arányban áll, további külön hozzájárulás nélkül, valamint az érintett hozzájárulásának visszavonását követően is kezelheti.

(4) Az adatkezelés megkezdése előtt az érintettet egyértelműen és részletesen tájékoztatni kell az adatai kezelésével kapcsolatos minden tényről, így különösen az adatkezelés céljáról és jogalapjáról, az adatkezelésre és az adatfeldolgozásra jogosult személyéről, az adatkezelés időtartamáról, illetve arról, hogy kik ismerhetik meg az adatokat, valamint arról, hogy az adatfelvétel kötelező vagy önkéntes. A tájékoztatásnak ki kell terjednie az érintett adatkezeléssel kapcsolatos jogaira és jogorvoslati lehetőségeire is. Kötelező adatfelvétel esetén a tájékoztatás megtörténhet a jelen pont szerinti információkat tartalmazó jogszabályi rendelkezésekre való utalás nyilvánosságra hozatalával is. Az Nftv. alapján kötelezően rögzítendő adatok körét a jelen Szabályzat 2. sz. melléklete tartalmazza.

(5) A tájékoztatás - különösen statisztikai vagy tudományos célú adatkezelés esetén - megtörténhet az előző bekezdésben meghatározott információknak mindenki számára hozzáférhető módon történő

be satisfied by the public disclosure of the information determined in the preceding paragraph.

(6) All personal data that are outside the sphere of mandatory reporting shall belong to voluntary reporting. That shall apply especially to data about the data subject's welfare situation and data that are needed to award allowances for students with outstanding academic accomplishments.

(7) Sensitive data may not be processed unless upon obtaining the data subject's written consent and in cases defined by law.

nyilvánosságra hozatalával is, ha az érintettek személyes tájékoztatás lehetetlen vagy aránytalan költséggel járna.

(6) Önkéntes adatszolgáltatás körébe tartozik minden, a kötelező adatszolgáltatás körén kívül eső személyes adat, így különösen a szociális helyzetre vagy kiemelkedő tanulmányi eredményre tekintettel adható kedvezmények megítéléséhez szükséges adatok.

(7) Különleges adat csak az érintett írásbeli hozzájárulásával vagy a vonatkozó jogszabályokban meghatározott esetekben kezelhető.

PART THREE Disclosure

Article 8

Personal data may be disclosed to third persons by transfer or by making public only pursuant to the provisions of Article 9 and 11 below.

Article 9

Disclosure Obligation

(1) Data may only be disclosed to a third party, whether it is a legal or a natural person, if that is authorized by law or, in its absence, if the data subject, having received appropriate information pursuant to the DPA, has authorized the University in writing to do so, provided that the conditions for data control are fulfilled in case of each personal data. The data subject may grant such authorization in advance either for a particular period or a certain circle of third party entities.

(2) Under the relevant legal provisions in force, personal data may be transferred for a

HARMADIK RÉSZ Adatközlés

8. §

Személyes adat harmadik személlyel adattovábbítás és nyilvánosságra hozatal keretében közölhető az alábbi 9.§, illetve 11.§-ok rendelkezéseivel összhangban.

9. §

Adattovábbítás

(1) Az Egyetemen kívüli szervtől vagy magánszemélytől érkező, adatközlésre irányuló megkeresés csak jogszabályi felhatalmazás esetében, illetve ilyen jogszabályi felhatalmazás hiányában csak akkor teljesíthető, ha az érintett az Info. tv.-ben meghatározott megfelelő tájékoztatás ismeretében, erre írásban felhatalmazza az Egyetemet, feltéve, hogy az adatkezelés feltételei minden egyes személyes adatra nézve teljesülnek. Az érintett előzetesen is adhat ilyen tartalmú felhatalmazást, amely szólhat valamely időtartamra és a megkereséssel élő szervek meghatározott körére.

(2) A hatályos jogszabályi rendelkezések értelmében az alábbi személyeknek

particular purpose without the data subject's consent in the following cases:

a) Data of the employees of the University – which are kept in registers of the University upon authorization of the law and which are listed in Appendix 2 attached to this Policy – may be transferred under the following conditions, except of the data indicated in Appendix 2, point (1) cm):

- the Maintainer may receive all of the data, commensurate to its needs to exercise its Maintainer's rights;
- entities that disburse social security benefits, consideration for work or other payments or rights may receive data they may need for deciding entitlement to any of the said sums;
- the entity that operates the information system of higher education may receive data that it may process under the NHEA;
- the Hungarian Accreditation Committee (MAB) may receive all data it needs for deciding whether or not the conditions for the operation of the higher education institution are there;
- the courts, the police, the prosecutor's office, bailiffs of the court, and agencies of public administration may receive data that they need for a decision in a concrete case;
- entities that have the right to inspect abidance with labor rules may receive data related to employment;
- the national security agencies may receive the data necessary for executing their tasks determined in Act CXXV of 1995 on national security agencies;
- to students or persons in work-related relationship with the higher education institution, the results of lecturer evaluation by students in the manner defined in the institutional bylaws; and
- pursuant to Section 28 of the DPA to applicants submitting a demand for

továbbíthatóak személyes adatok - célhoz kötötten - az érintett hozzájárulása nélkül:

a) Az Egyetem alkalmazottainak a jelen szabályzat 2. sz. mellékletében felsorolt, törvényi felhatalmazás alapján nyilvántartott adatai – a jelen Szabályzat 2. sz. mellékletének (1) cm) pontja szerinti adatok kivételével - továbbíthatók:

- a fenntartónak valamennyi adat, a fenntartói jogok gyakorlásához szükséges mértékben;
- a társadalombiztosítási, illetmény és munkabér vagy más juttatás, jogosultság kifizetőhelyének minden olyan adat, amely az illetmény, munkabér vagy más juttatás, jogosultság megállapításához, igénybeviteléhez szükséges;
- az felsőoktatási információs rendszer működéséért felelős szervnek minden olyan adat, amelyet az Nftv. szerint a felsőoktatási információs rendszer kezelhet;
- a Magyar Felsőoktatási Akkreditációs Bizottságnak minden olyan adat, amely ahhoz szükséges, hogy megállapíthassa a felsőoktatási intézmény működéséhez szükséges feltételek meglétét;
- a bíróságnak, rendőrségnek, ügyészségnek, a bírósági végrehajtónak, államigazgatási szervnek a konkrét ügy eldöntéséhez szükséges adatok;
- a munkavégzésre vonatkozó rendelkezések ellenőrzésére jogosultaknak a foglalkoztatással összefüggő adatok,
- a nemzetbiztonsági szolgálatnak a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvényben („Nbtv.”) meghatározott feladatok ellátásához szükséges valamennyi adat;
- az oktatói munka hallgatói véleményezése eredményeit a felsőoktatási intézménnyel hallgatói, foglalkoztatási jogviszonyban állók számára az intézményi szabályzatban meghatározott módon; valamint
- az Info tv. 28. § alapján a felsőoktatási intézményhez intézett adat-megismerési

accessing data to a higher education institution all data qualified as data of public interest in Section 26 (3) of the DPA.

b) The following data of the students – kept in accordance with the law in registers of the University and listed in Appendix 2 attached to this Policy – may be disclosed as follows:

- the Maintainer may receive all of the data that are related to its Maintainer's functions;
- the courts, the police, the prosecutor's office, bailiffs of the court, and agencies of public administration may receive data that they need for a decision in a specific case;
- the national security agencies may receive all data necessary for executing their tasks determined in Act CXXV of 1995 on national security agencies;
- the entity that operates the information system of higher education may receive all data;
- the Student Loan Centre may receive data related to the person inquiring student loan, as determined in the NHEA,
- the institution responsible for registering the fulfillment of the Hungarian state scholarship, may receive data related to the programs and student status.

(3) Data that are not mentioned in paragraph (2) above may only be disclosed with the data subject's consent provided the preconditions for data processing are there for each of the personal data.

(4) Personal data may be transmitted by the University to a data controller operating in a third country, or may be disclosed to a data controller or processor operating in a third country if:

- a) the data subject has given his/her explicit consent, or
- b) the legal conditions for data processing are satisfied and - save where Subsection (2) of Section 6 of the DPA applies - the laws of the third country in question afford an adequate level of protection with respect to the control

kérelem teljesítése céljából a kérelmezőnek az Info tv. 26. § (3) bekezdése szerinti közérdekből nyilvános adatként minősülő adatok.

b) A hallgatók 2. sz. mellékletben felsorolt, törvényi felhatalmazás alapján nyilvántartott adatai továbbíthatók:

- a fenntartónak valamennyi adat, a fenntartói irányítással összefüggő feladatok ellátásához;
- a bíróságnak, rendőrségnek, ügyészségnek, a bírósági végrehajtónak, államigazgatási szervnek a konkrét ügy eldöntéséhez szükséges adat;
- a nemzetbiztonsági szolgálat részére az Nbtv.-ben meghatározott feladatok ellátásához szükséges valamennyi adat;
- a felsőoktatási információs rendszer működéséért felelős szerv részére valamennyi adat;
- a Diákhitel Központnak a hallgatói hitelt igényelt személyekhez kapcsolódóan, az Nftv.-ben meghatározott adatok,
- a magyar állami ösztöndíj feltételei teljesítésének nyilvántartásáért felelős szervnek a képzésre és a hallgatói jogviszonyra vonatkozóan.

(3) A (2) bekezdésben nem nevesített adatok csak az érintett hozzájárulásával és csak abban az esetben továbbíthatók, ha az adatkezelés feltételei minden egyes személyes adatra teljesülnek.

(4) Személyes adatot az Egyetem az Egyetem által megbízott adatfeldolgozó harmadik országban adatkezelést folytató adatkezelő részére akkor továbbíthat, vagy harmadik országban adatfeldolgozást végző adatfeldolgozó részére akkor adhat át, ha

- a) ahhoz az érintett kifejezetten hozzájárult, vagy
- b) az adatkezelésnek a jogszabályai feltételei teljesülnek, és – az Info tv. 6. § (2) bekezdésében foglalt esetet kivéve - a harmadik országban az átadott adatok kezelése, valamint feldolgozása során

and processing of the personal data transmitted. Transmission of data to EEA Member States shall be treated as if the transmission took place within the territory of Hungary.

(5) Data may be transmitted by the Rector of the University (acting as the head of the University), other senior official or member of the staff authorized by him – as defined by the authorization.

(6) The person who transmits data shall inform the Internal Data Protection Officer about the data transmitted, the purpose and addressee of data transmission, and all other circumstances that are relevant for data transmission. The Internal Data Protection Officer shall keep a register of the data transmitted (Data Transmission Register). The register may be integrated with the register to be kept about data control.

Article 10

Combination of Data

(1) Data control that is done at the University for various purposes may only be connected upon obtaining the consent of the data subject or when processing is necessary as decreed by law, provided the preconditions for processing each of the personal data and for each part of processing are met.

(2) The planned connection of data control for the purpose of making the register of data control up to date, shall be communicated to the Internal Data Protection Officer by a reasonable time before actual execution.

biztosított a személyes adatok megfelelő szintű védelme. Az EGT-államba irányuló adattovábbítást úgy kell tekinteni, mintha Magyarország területén belüli adattovábbításra kerülne sor.

(5) Adattovábbításra az Egyetem rektora (mint az Egyetem vezetője), az általa meghatalmazott vezető vagy más alkalmazott jogosultak – a meghatalmazás keretei között.

(6) Az adattovábbítást végző személy a továbbított adatokról, az adattovábbítás céljáról és címzettjéről, valamint az adattovábbítás szempontjából jelentős valamennyi körülményről tájékoztatja a belső adatvédelmi felelőst. A belső adatvédelmi felelős a továbbított adatokról adattovábbítási nyilvántartást vezet (Adattovábbítási nyilvántartás), amely nyilvántartás az adatkezelések nyilvántartásával összevontan is vezethető.

10. §

Adatok összekapcsolása

(1) Az Egyetemen folyó különböző célra irányuló adatkezelések csak az érintettek hozzájárulása esetén, vagy törvényi felhatalmazás alapján kapcsolhatók össze, ha az adatkezelés feltételei minden egyes személyes adatra és az adatkezelés minden részműveletére nézve teljesülnek.

(2) Az adatkezelések tervezett összekapcsolását az adatkezelési nyilvántartás napra készen tartása érdekében a belső adatvédelmi felelősnek a tervezett intézkedés elvégzését megelőző ésszerű időn belül, előre be kell jelenteni.

Article 11

Public Disclosure of Data

(1) It is forbidden to disclose the personal data processed by the University unless that is authorized by an Act or consented by the data subject.

(2) Data that cannot be brought into relation with any particular natural persons may be transferred without limitations or disclosed by the persons responsible for data control under the authorization of the Rector or the Internal Data Protection Officer.

PART FOUR

Article 12

The Data Subjects' Rights, Ensuring the Right to Informational Privacy

(1) A data subject may,
(i) request information from the University about the processing of his/her personal data,
(ii) request the rectification of his/her personal data,
(iii) request the erasure or blocking of his personal data, save where processing is rendered mandatory, and
(iv) may request access to that part of the registers where his/her personal data are stored. Inspection shall be ensured in such a way so that the data subject should not have access to the personal data of others.

(2) In case a data subject so requires, he/she must be given information about his/her personal data as processed by the University, including those processed by a data processor hired by the University or by others based on its instructions, the sources from where they were obtained, the duration and purposes of and the legal grounds for processing his/her personal data, about personal data that have been processed by a technical data processor commissioned by the University, the name and address (seat) of the technical data

11. §

Nyilvánosságra hozatal

(1) Az Egyetem által kezelt személyes adatok nyilvánosságra hozatala – törvényi felhatalmazás vagy az érintett hozzájárulásának hiányában – tilos.

(2) A meghatározott természetes személlyel kapcsolatba nem hozható adatok a rektor vagy a belső adatvédelmi felelős felhatalmazása alapján az adatkezelésért felelős személyek által korlátozás nélkül továbbíthatóak, illetve nyilvánosságra hozhatóak.

NEGYEDIK RÉSZ

12. §

Az érintettek jogai, az információs önrendelkezési jog biztosítása

(1) Az érintett az Egyetemtől
(i) tájékoztatást kérhet személyes adatainak kezeléséről,
(ii) kérheti személyes adatainak helyesbítését,
(iii) kérheti személyes adatainak törlését vagy zárolását, a kötelező adatkezelés kivételével, valamint
(iv) a nyilvántartás róla szóló részébe betekinhet. A betekintést úgy kell biztosítani, hogy az érintett más személy adatait ne ismerhesse meg.

(2) Kérésre az érintettet tájékoztatni kell az Egyetem által kezelt, illetve az Egyetem által vagy az Egyetem rendelkezése szerint megbízott adatfeldolgozó által feldolgozott adatairól, azok forrásáról, az adatkezelés időtartamáról, céljáról, jogalapjáról, illetőleg az Egyetem által megbízott adatfeldolgozó által feldolgozott adatairól, az adatfeldolgozó nevééről, címéről (székhelyéről) és az adatkezeléssel összefüggő tevékenységéről, továbbá arról, hogy kik és milyen célból kapják vagy

processor and his/her activities related to data processing, furthermore, on who have received his/her personal data and for what purposes, and other circumstances that are related to data control and are defined by law.

(3) When a data is rectified, blocked, marked or erased, the data subject to whom it pertains and all recipients to whom it was transmitted for processing shall be notified. Notification is not required if it does not violate the rightful interest of the data subject in light of the purpose of processing.

(4) If the University refuses to comply with the data subject's request for rectification, blocking or erasure, the factual or legal reasons on which the decision for refusing the request for rectification, blocking or erasure is based shall be communicated in writing, or - with the data subject's consent - electronically, within twenty-five days of the receipt of the request. Where rectification, blocking or erasure is refused, the University shall inform the data subject of the possibilities for seeking judicial remedy or lodging a complaint with the Authority.

(5) The data subject may protest at the processing of his/her personal data in cases, and in a manner, defined by Article 21 of the DPA.

kapták meg az adatokat, valamint az adatkezeléssel összefüggő, jogszabályban meghatározott egyéb tényekről is.

(3) A helyesbítésről, a zárolásról, a megjelölésről és a törlésről az érintettet, továbbá mindazokat értesíteni kell, akiknek korábban az adatot adatkezelés céljára továbbították. Az értesítés mellőzhető, ha ez az adatkezelés céljára való tekintettel az érintett jogos érdekét nem sérti.

(4) Ha az adatkezelő az érintett helyesbítés, zárolás vagy törlés iránti kérelmét nem teljesíti, a kérelem kézhezvételét követő 25 napon belül írásban vagy az érintett hozzájárulásával elektronikus úton közli a helyesbítés, zárolás vagy törlés iránti kérelem elutasításának ténybeli és jogi indokait. A helyesbítés, törlés vagy zárolás iránti kérelem elutasítása esetén az adatkezelő tájékoztatja az érintettet a bírósági jogorvoslat, továbbá a Hatósághoz fordulás lehetőségéről.

(5) Az érintett az Info tv. 21. §-ban meghatározott esetben és módon tiltakozhat személyes adatának kezelése ellen.

PART FIVE

Provisions on Data Security

Article 13

In accordance with the requirements on data security, the University shall make arrangements for and carry out data control operations in a way so as to ensure full respect for the right to privacy of data subjects in due compliance with the provisions of the DPA and other regulations on data protection. The University shall take the technical and organizational measures, and shall develop the rules of procedure, that are needed to ensure that the provisions of the NHEA, the

ÖTÖDIK RÉSZ

Adatbiztonsági rendelkezések

13. §

Az adatbiztonság követelményének megfelelően, az Egyetem köteles az adatkezelési műveleteket úgy megtervezni és végrehajtani, hogy az az Info. tv. és az adatkezelésre vonatkozó más szabályok alkalmazása során biztosítsa az érintettek magánszférájának védelmét. Az Egyetem megteszi azokat a technikai és szervezési intézkedéseket, valamint kialakítja azokat az eljárási szabályokat, amelyek az Nftv. és az Info. tv. rendelkezéseinek és minden egyéb,

DPA and other relevant legal provisions on data protection should be enforced. The data shall be protected especially from unlawful access, alteration, transfer, publication, deletion or destruction, and accidental annihilation or damage and to ensure that stored data cannot be corrupted and rendered inaccessible due to any changes in or modification of the applied technique.

Article 14

Protection of Electronically Stored Data

For the protection of data sets stored in different electronic filing systems, suitable technical solutions shall be introduced to prevent - unless this is permitted by law - the interconnection of data stored in these filing systems and the identification of the data subjects. Electronically stored data shall be protected in particular against

- environmental damage (fire, water, dust, etc.);
- virus attacks;
- unauthorized backup;
- unauthorized archiving;
- access by unauthorized persons.

Article 15

Protection of Data Stored on Paper

Data stored on paper shall be protected in particular against

- environmental damage (fire, water, dust, etc.);
- unauthorized multiplication,
- unauthorized archiving;
- unauthorized access by unauthorized persons.

vonatkozó jogszabály előírásainak érvényre juttatásához szükségesek. Az adatokat védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen.

14. §

Elektronikusan tárolt adatok védelme

A különböző nyilvántartásokban elektronikusan kezelt adatállományok védelme érdekében az Egyetem megfelelő technikai megoldással biztosítja, hogy a nyilvántartásokban tárolt adatok – kivéve, ha azt törvény lehetővé teszi - közvetlenül ne legyenek összekapcsolhatók és az érintetthez rendelkezhetők. Az elektronikusan tárolt adatok védelmét biztosítani szükséges különösen az alábbi behatásoktól:

- környezeti behatások (tűz-, víz-, por-, stb. elleni védelem);
- vírusvédelem;
- adatok illetéktelen biztonsági mentése;
- illetéktelen archiválás;
- illetéktelen személyek általi hozzáférés.

15. §

Papíralapon tárolt adatok védelme

A papíralapú adatok védelmét biztosítani szükséges különösen az alábbi behatásoktól:

- környezeti behatások (tűz-, víz-, por-, stb. elleni védelem);
- adatok illetéktelen sokszorozása;
- illetéktelen archiválás;
- illetéktelen személyek általi hozzáférés kizárása.

PART SIX

Inspection, the Functions of the Internal Data Protection Officer

Article 16

(1) The Rector of the University shall have the right to inspect the compliance with the rules of personal data protection. In case the Rector discovers a violation of the rules of personal data protection, he shall take steps without delay to terminate that violation and inform the Internal Data Protection Officer.

(2) The Rector of the University shall, within eight days of the announcement of this Policy, appoint from the employees of the University an Internal Data Protection Officer for the duration of two years. The Internal Data Protection Officer shall inspect the enforcement of the Personal Data Protection Policy and, if needed, recommend its revision. The Internal Data Protection Officer shall treat as confidential the data he/she has access to during his/her work. The name and availability of the Internal Data Protection Officer are indicated in Appendix 1.

(3) The Internal Data Protection Officer is entitled to inspect the work of all data processing officials who keep the University's registers. In that capacity the Internal Data Protection Officer may

- have access to the University's registers and copy them;
- request oral or written information from persons responsible for data control and technical data processors who process data as commissioned by the data controller;
- temporarily take possession of the University's registers without interfering with their proper use.

(4) To comply with this Policy and the relevant laws, the Internal Data Protection

HATODIK RÉSZ

Ellenőrzés, a belső adatvédelmi felelős

16. §

(1) Az adatvédelmi szabályok betartásának ellenőrzésére az Egyetem rektora jogosult. Amennyiben a rektor az adatvédelmi szabályok megsértését észleli, haladéktalanul köteles a sérelem megszüntetése érdekében eljárni, valamint a belső adatvédelmi felelőst értesíteni.

(2) A jelen Szabályzat érvényesülésének ellenőrzésére és esetleges felülvizsgálatának kezdeményezésére 2 évre az Egyetem rektora belső adatvédelmi felelőst nevez ki a jelen Szabályzat kihirdetését követő 8 napon belül az egyetem dolgozói közül. A belső adatvédelmi felelőst a megismert adatokkal kapcsolatban titoktartási kötelezettség terheli. A belső adatvédelmi felelős mindenkori személyét és elérhetőségét a jelen szabályzat 1. számú melléklete tartalmazza.

(3) A belső adatvédelmi felelős jogosult minden, az egyetemi nyilvántartások vezetésére kijelölt adatkezelésért felelős személy tevékenységének ellenőrzésére. Ennek keretében a belső adatvédelmi felelős jogosult:

- az Egyetem nyilvántartásaiba betekinteni, azokról másolatot készíteni;
- az adatkezelésért felelős személyektől, illetve az adatkezelő megbízása alapján adatfeldolgozást végző adatfeldolgozóktól szóban vagy írásban tájékoztatást kérni;
- az Egyetem nyilvántartásait átmenetileg és a rendeltetésszerű használatot nem zavaró módon magához venni.

(4) A belső adatvédelmi felelős a jelen szabályzatnak és a törvényi

Officer shall examine the work of every person responsible for data control and every register at least once a year. The Internal Data Protection Officer shall give feedback about his/her inspection for the person he/she has examined. In case the Internal Data Protection Officer notices some violation of the data controlling rules, he/she shall call the attention of the person responsible for data control to adhere to the rules.

(5) The Internal Data Protection Officer shall:
a) participate and assist in the decision-making process with regard to data control and enforcing the rights of data subjects;

b) monitor compliance with the provisions of the DPA and other regulations on data processing as well as with the provisions of internal data protection and data security regulations and the data security requirements;

c) investigate complaints conveyed to him/her and, if he/she detects any unauthorized data control operations, call on the controller or processor in question to cease such operations;

d) draw up the internal data protection and data security rules;

e) maintain the internal data protection register;

f) arrange training sessions on the subject of data protection.

rendelkezéseknek való megfelelés érdekében évente legalább egyszer köteles minden adatkezelésért felelős személy és nyilvántartás ellenőrzésére. Az ellenőrzés eredményéről az ellenőrzött részére a belső adatvédelmi felelős visszaigazolást ad. Az adatkezelési szabályok megszegésének észleli, felhívja az adatkezelésért felelős személyt az előírásoknak megfelelő adatkezelésre.

(5) A belső adatvédelmi felelős

a) közreműködik, illetve segítséget nyújt az adatkezeléssel összefüggő döntések meghozatalában, valamint az érintettek jogainak biztosításában;

b) ellenőrzi az Info. tv. törvény és az adatkezelésre vonatkozó más jogszabályok, valamint a belső adatvédelmi és adatbiztonsági szabályzatok rendelkezéseinek és az adatbiztonsági követelményeknek a megtartását;

c) kivizsgálja a hozzá érkezett bejelentéseket, jogosulatlan adatkezelés észlelése esetén annak megszüntetésére hívja fel az adatkezelőt vagy az adatfeldolgozót;

d) elkészíti a belső adatvédelmi és adatbiztonsági szabályzatot;

e) vezeti a belső adatvédelmi nyilvántartást;

f) gondoskodik az adatvédelmi ismeretekoktatásáról.

PART SEVEN

Internal Registration of Data Control

Article 17

(1) Prior to controlling personal data, and prior to start using a new register system, the head of the organizational unit that is responsible for data processing shall notify the Internal Data Protection Officer. Such notice shall indicate

a) the purpose of and legal justification for the planned data control;

HETEDIK RÉSZ

Az adatkezelések belső nyilvántartása

17. §

(1) A személyes adatok kezelésének megkezdése és új nyilvántartó rendszer alkalmazásba vétele előtt az adatkezelésért felelős szervezeti egység vezetőjének értesítenie kell a tervezett adatkezelésről a belső adatvédelmi felelőst. Az értesítésben meg kell jelölni a

a) a tervezett adatkezelés célját és jogalapját;

b) the information technology characteristics of the planned register system;
c) the fact that the planned system or data control shall replace an earlier system or data control.

(2) Having received a notice in compliance with paragraph (1) above, the Internal Data Protection Officer shall examine whether or not the legal justification and the purpose of the planned data control or register system complies with the provisions of the NHEA and the DPA and of other legal provisions on data protection and whether it is necessary to enter the planned data processing into the data protection register.

(3) In case in the opinion of the Internal Data Protection Officer the planned data control does not comply with the provisions of the NHEA and the DPA and of other legal provisions on data protection with respect to its legal justification or for some other reason, he/she shall notify the head of the organizational unit concerned and initiates a consultation. Until such discussion has not been successfully completed, or in the absence of full compliance with the legal provisions referred to in this paragraph, data control shall not commence, and the register system shall not enter use. The same procedure shall be applied whenever an internal dispute may arise on how to interpret the provisions of this Policy.

(4) In case in the opinion of the Internal Data Protection Officer the planned data control – especially as far as its purpose and legal justification are concerned – complies with the provisions of the NHEA, the DPA and other provisions on data protection, then the Internal Data Protection Officer shall fill in a form (see Appendix 3 attached to this Policy), and he/she shall enter it into the internal data processing register. If need be, the Internal Data Protection Officer shall notify the data protection register and notify the Authority about the processing of a new data file and the use of a new technique for data processing.

b) a tervezett nyilvántartó rendszer informatikai jellemzőit;
c) azt a tényt, hogy a tervezett rendszer vagy adatkezelés valamely korábbi rendszer vagy adatkezelés helyére lép.

(2) A belső adatvédelmi felelős az (1) szakaszban szabályozott értesítés nyomán megvizsgálja, hogy a tervezett adatkezelés vagy nyilvántartó rendszer jogalapja, a cél meghatározása megfelel-e az Nftv. és az Info. tv. rendelkezéseinek és az egyéb adatvédelmi jogszabályok előírásainak, és szükséges-e az adatkezelésnek az adatvédelmi nyilvántartásba történő bejelentése.

(3) Ha a belső adatvédelmi felelős szerint az adatkezelés céljának meghatározása, jogalapja vagy más ok miatt nem felel meg az Nftv. és az Info. tv. rendelkezéseinek és az egyéb adatvédelmi jogszabályok előírásainak, értesíti az érintett szervezeti egység vezetőjét, és egyeztetést kezdeményez. Az egyeztetés sikeres lezárásáig, illetve a jelen pontban hivatkozott, vonatkozó jogszabályoknak való teljeskörű megfelelés hiányában az adatkezelés nem kezdhető meg, illetve a nyilvántartó rendszer nem vehető alkalmazásba. Ez a hatásköri szabály alkalmazandó minden, a jelen szabályzat alkalmazása során felmerülő belső jogalkalmazási vita eldöntésénél is.

(4) Ha a belső adatvédelmi felelős álláspontja szerint az adatkezelés – különösen a cél meghatározása és a jogalap – megfelel az Nftv. és az Info. tv. rendelkezéseinek és az egyéb adatvédelmi jogszabályok előírásainak, akkor a jelen szabályzat 3. sz. melléklete szerinti adatkezelési adatlapot állít ki, és azt elhelyezi az általa vezetett belső adatkezelési nyilvántartásban. A belső adatvédelmi felelős szükség esetén megteszi a szükséges bejelentést az adatvédelmi nyilvántartásba, illetve értesíti az új adatállomány feldolgozásáról vagy az új adatfeldolgozási technológia alkalmazásáról a Hatóságot.

(5) In case it is planned to discontinue processing personal data or shutting down a register system, the head of the organizational unit in charge of data control shall notify the Internal Data Protection Officer in a reasonable time ahead of taking any of those measures.

(6) It shall be the responsibility of the Internal Data Protection Officer to keep a register of the data control sheets (internal data protection register). The register may also be processed in an electronic form. Only the Internal Data Protection Officer shall have the right to enter data into the register. Whenever a correction or deletion is done, the corrected or deleted data, and the date when the correction or deletion occurred, shall remain a part of the register in a readable form. The Internal Data Protection Officer shall begin keeping a data control sheet about data control that is required by the law, and shall enter it into the register, within 90 days of this Policy entering into force.

(7) Upon the data subject's request the University shall provide information concerning the data relating to him/her, including those processed by a data processor hired by the University or by others based on its instructions, the sources from where they were obtained, the purpose, grounds and duration of processing, the name and address of the data processor and on its activities relating to data processing, the circumstances surrounding the privacy incident, its impact, and the actions taken to rectify the situation, and - if the personal data of the data subject is transferred - the legal basis and the recipients.

(8) The University shall keep records - by way of an internal data protection officer where applicable - for the purpose of monitoring actions taken in connection with privacy incidents and for information of the public and of data subjects, containing the data subjects' personal data, the data subjects

(5) Valamely személyes adatkezelés vagy nyilvántartó rendszer megszüntetése esetén az adatkezelésért felelős szervezeti egység vezetőjének a tervezett intézkedést megelőző ésszerű időn belül értesítenie kell a belső adatvédelmi felelőst. A belső adatvédelmi felelős feltünteti a belső adatkezelési nyilvántartásban az adatkezelés megszüntetését.

(6) Az adatkezelési lapok nyilvántartásának (belső adatvédelmi nyilvántartás) vezetése a belső adatvédelmi felelős feladata. A nyilvántartás elektronikus formában is kezelhető. A nyilvántartásba bejegyzést csak a belső adatvédelmi felelős tehet. A javítás, törlés oly módon történik, hogy a javított illetve törölt bejegyzés, valamint azok elvégzésének időpontja, olvasható módon a nyilvántartás része marad. A jogszabályban elrendelt adatkezelésekről jelen szabályzat hatálybalépésétől számított 90 napon belül kell a belső adatvédelmi felelősnek nyilvántartási lapot felvenni, és azt a nyilvántartásban elhelyezni.

(7) Az érintett kérelmére az Egyetem tájékoztatást ad az érintett általa kezelt, illetve az általa vagy rendelkezése szerint megbízott adatfeldolgozó által feldolgozott adatairól, azok forrásáról, az adatkezelés céljáról, jogalapjáról, időtartamáról, az adatfeldolgozó nevééről, címéről és az adatkezeléssel összefüggő tevékenységéről, az adatvédelmi incidens körülményeiről, hatásairól és az elhárítására megtett intézkedésekről, továbbá - az érintett személyes adatainak továbbítása esetén - az adattovábbítás jogalapjáról és címzettjéről.

(8) Az Egyetem a belső adatvédelmi felelős útján az adatvédelmi incidenssel kapcsolatos intézkedések ellenőrzése, valamint az érintett tájékoztatása céljából nyilvántartást vezet, amely tartalmazza az érintett személyes adatok körét, az adatvédelmi incidenssel érintettek körét és számát, az

involved and their number affected by the privacy incident, the time when the privacy incident took place, its circumstances and impacts, the actions taken to rectify the situation, and other data provided for in the legislation on data processing (Privacy incident register).

adatvédelmi incidens időpontját, körülményeit, hatásait és az elhárítására megtett intézkedéseket, valamint az adatkezelést előíró jogszabályban meghatározott egyéb adatokat (Adatvédelmi incidens nyilvántartás).

PART EIGHT

NYOLCADIK RÉSZ

Use of Data for Purposes of Scientific Research

Tudományos kutatási célú adatkezelés

(1) Scientific researchers, prior to commencing the research projects under the scope of the Research Data Control Act, must prepare a *data control plan*. Such plan is to be modified if the purpose of the data use is changed during the research process. The plan of research oriented data use must include:

- a) the entitlement to conduct research,
- b) the objective of the research,
- c) the source and sphere of personal data to be used,
- d) the process of data use,
- e) guarantees for practical enforcement of the subject party's rights, and
- f) the technical and organisational measures taken for data protection.

(2) The data control plan shall be kept on file in order to provide proof of the legitimacy of the data use and for inspection until the use of the data is terminated.

(3) In the case of institutional scientific research projects, the rights and obligations of the scientific researcher shall fall on and are to be observed by the organisation carrying out the research activity.

(4) In the use of data for scientific research, public opinion surveys, market research and direct marketing purposes - in accordance with the provisions of the DPA and of the Research Data Control Act - the right of the

(1) A tudományos kutatónak a Kutatási Adatkezelési tv. hatálya alá tartozó kutatás megkezdése előtt *kutatási adatkezelési tervet* kell készítenie. A tervet módosítani kell, ha az adatkezelés célja a kutatás folyamata alatt megváltozik.

A kutatási adatkezelési tervnek tartalmaznia kell:

- a) a kutatási jogosultságot,
- b) a kutatás célját,
- c) a kezelendő személyes adatok körét és azok forrását,
- d) az adatkezelés folyamatát,
- e) az érintett jogai gyakorlati érvényesíthetőségének biztosítékait, valamint
- f) az adatvédelmet biztosító technikai és szervezési intézkedéseket.

(2) A kutatási adatkezelési tervet az adatkezelés jogszerűségének bizonyíthatósága és az ellenőrzés lehetőségének biztosítása céljából az adatok kezelésének megszűntetéséig meg kell őrizni.

(3) Intézeti tudományos kutatás esetén a tudományos kutató jogait és kötelezettségeit a kutatási tevékenységet végző szervezet illetik meg, illetőleg terhelik.

(4) A tudományos kutatás, a közvélemény-kutatás és piackutatás, valamint a közvetlen üzletszerzés céljára történő adatkezelés során - az Info. törvényben, valamint a Kutatási Adatkezelési törvényben

subject party to the protection of his personal data shall have to be provided. Particularly in regard to the following:

a) at the time of establishing contact, the subject party is to be informed in writing of the source of information on him used by the contacting person; on the objective, method and duration of using the data, on the use of a mediator (agent) during data use, and on any future intent to transfer such data; on the name and address of the organisation or person entitled to use, and on the fact that supplying data is voluntary and that the subject party has the right to request that his data should not be used for the designated purpose or portions of such purpose;

b) the subject party must be ensured the right to deny any further co-operation without explanation, and is to be informed of such right in writing;

c) the use of the subject party's name and address information for the purposes as defined in the Research Data Control Act is to be terminated, if so requested by the subject party, or if said subject party does not consent to the use of his data;

d) the subject party's name and address information may only be transferred with his/her written consent, with the exception of transferring data as defined in Paragraph c) of subsection (1) of Section 3 of the Research Data Control Act, of data processing by consignment, and data conformation specified in this same Act [subsection (3) of Section 4].

(5) When transferring data, both sides must keep records on the opposite party and the relevant data transferred in order to make such suitable for inspection. Such records are to be kept on file for five years from the date of transfer. When processing data on consignment, the employer shall be considered as the responsible party for data use.

foglaltaknak megfelelően - biztosítani kell az érintett jogát a személyes adatainak védelméhez. Így különösen:

a) a kapcsolatfelvétellel egyidejűleg az érintettet írásban tájékoztatni kell arról, hogy a megkereső az adatokat milyen forrásból szerezte; az adatfelhasználás céljáról, módjáról, időtartamáról, az adatkezelés során közreműködő (megbízott) igénybevételéről és az esetleges későbbi adatátadási szándékról; az adatkezelésre jogosult szerv vagy személy nevééről és címéről, valamint arról, hogy az adatszolgáltatás önkéntes, és jogában áll adatainak a megjelölt célra vagy annak egy részére történő kezelésének a megszüntetését kérni;

b) biztosítani kell számára azt a jogot, hogy a további együttműködést bármikor indokolás nélkül megtagadhatja, és erről írásban tájékoztatni kell;

c) név- és lakcímadatainak a Kutatási Adatkezelési törvényben meghatározott tevékenységek céljából történő kezelését meg kell szüntetni, amennyiben ezt az érintett kéri, vagy adatainak kezeléséhez nem járul hozzá;

d) név- és lakcímadatait harmadik személynek vagy szervezetnek továbbítani – a Kutatási Adatkezelési törvény 3. § (1) bekezdés c) pontja alapján történő adattovábbítás, a megbízás alapján történő adatfeldolgozás, valamint az ugyanezen törvényben meghatározott adategyeztetés [4. § (3) bekezdése] kivételével - csak az érintett írásbeli hozzájárulásával lehet.

(5) Adatátadás esetén mind az adatátadónak, mind az - átvevőnek az érintett adatokról és az adatátvevőről, illetőleg - átadóról - az adatforgalom ellenőrizhetőségének biztosítása céljából - nyilvántartást kell vezetni. A nyilvántartást az adatátvétel, illetve az adatátadás évét követő ötödik év végéig kell megőrizni. A megbízás alapján történő adatfeldolgozás esetén a megbízó minősül felelős adatkezelőnek.

(6) The use of personal data for specific objectives must be terminated, if
a) the objective for which the data was requested has been attained, unless the subject party has given his consent to further use of data for a new objective;
b) the subject party has declared that he/she does not wish to co-operate with the contact organisation.

(6) A személyes adatoknak az adott célból történő kezelését meg kell szüntetni, ha
a) az a cél, amelyre az adatokat kérték megvalósult, kivéve, ha az érintett az új cél megjelölésével az adatok további kezeléséhez írásban hozzájárult;
b) az érintett nyilatkozata szerint a megkereső szervezettel nem kíván együttműködni.

(7) Termination of data processing shall be construed as the data is erased or made anonymous, while in respect to direct marketing - if such termination is based on Paragraph b) of Subsection (3) of the Research Data Control Act - it also means the inclusion of such data on the prohibitive list described in Section 21.

(7) Az adatkezelés megszüntetésén a megsemmisítést vagy az anonimizálást, közvetlen üzletszerzés esetén pedig - ha a megszüntetés a Kutatási Adatkezelési törvény (3) bekezdés b) pontján alapul - egyidejűleg a 21. § szerinti tilalmi listára történő felvételt kell érteni.

(8) If the use of data is to be terminated at any stage on request of subject party, subject party shall not be held responsible for such termination.

(8) Ha az adatkezelést annak bármely szakaszában az érintett kérelme alapján kell megszüntetni, ezért az érintettet jogi felelősség nem terheli.

PART NINE

KILENCEDIK RÉSZ

Surveillance Cameras

Biztonsági kamerák

Article 18

18. §

(1) The University shall notify future students in the admission brochures that in certain places of the University complex surveillance cameras have been installed exclusively for the purpose of protecting persons and property and in accordance with the relevant legal provisions.

(1) Az Egyetem minden jövőbeli hallgatójának szóló felvételi tájékoztatóban utal arra, hogy az Egyetem területén kizárólag személy- és vagyonvédelmi célból a hatályos jogszabályi rendelkezések keretei között, az abban előírt feltételek mellett, meghatározott helyeken biztonsági kamerák működnek.

(2) Those affected by the operation of surveillance cameras may exercise their rights in ways and in consideration of deadlines that are defined by law. The Internal Data Protection Officer shall inform those affected about the relevant legal provisions upon request.

(2) Az érintettek a biztonsági kamerák működésével összefüggésben a jogszabályban meghatározott módon és határidők mellett gyakorolhatják jogukat, amelyekről a belső adatvédelmi felelős az érintett kérelmére tájékoztatást ad.

PART TEN

Closing Provisions

Article 19

(1) The specific rules related to the processing of personal data are regulated in separate Data Processing Information. The sample Data Processing Information is attached to this Policy as Appendix 5.

(2) Matters that are not covered by this Policy shall be governed by the relevant laws, especially the relevant provisions of the NHEA and the DPA as well as other data protection rules.

(3) The present Policy will come into force upon approval by the University's Senate.

Budapest, May 29, 2017

**A Közép-európai Egyetem nevében /
On behalf of the Közép-európai Egyetem
aláírta:**

**Michael Ignatieff
Rector / Rektor**

**A Central-European University, New York
névében aláírta**

**On behalf of Central-European University,
New York signed by:
Michael Ignatieff
President and Rector**

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

TIZEDIK RÉSZ

Záró rendelkezések

19. §

(1) Az egyes személyes adatok kezelésére vonatkozó speciális szabályok külön Adatvédelmi Tájékoztatókban kerülnek rögzítésre. Az Adatvédelmi Tájékoztató mintája a jelen Szabályzat 5. sz. mellékletét képezi.

(2) A jelen Szabályzatban nem szabályozott kérdések tekintetében a vonatkozó jogszabályok, így különösen az Nftv. és az Info. tv., valamint az adatvédelmi tárgyú terület-specifikus jogszabályok vonatkozó rendelkezései az irányadóak.

(3) A jelen szabályzat a Szenátus által történő elfogadás napján lép hatályba.

Budapest, 2017. május 29.

**A Fenntartó nevében aláírta/ On
behalf of the Maintainer signed by :**

**Liviu Matei,
a Budapesti Közép-európai Egyetem
Alapítvány meghatalmazottja/
Authorized representative of the
Central European University
Foundation of Budapest**

Appendices:

Appendix 1: Positions with responsibilities related to data control

Appendix 2: Personal and sensitive data kept and processed by higher education institutions

Appendix 3: Form on the University's internal data protection register

Appendix 4: Summary of the legal provisions on the consequences of violating the rules of personal data control

Appendix 5: Information on the available legal remedies

Appendix 6: Information on Data Processing (SAMPLE)

Appendix 7: Privacy Incident Register (SAMPLE)

Appendix 8: Data Transmission Register (SAMPLE)

Mellékletek:

1. sz. melléklet: Adatkezelésért felelős munkakörök

2. sz. melléklet: A felsőoktatási intézményekben nyilvántartott és kezelt személyes és különleges adatok

3. sz. melléklet: Adatlap az Egyetem belső adatvédelmi nyilvántartásához

4. sz. melléklet: A személyes adatok kezelésére vonatkozó szabályok megsértésére vonatkozó jogkövetkezmények (a vonatkozó jogszabályi előírások) összefoglalása

5. sz. melléklet: Tájékoztató a jogorvoslati lehetőségekről

6. sz. melléklet: Adatvédelmi tájékoztató (MINTA)

7. sz. melléklet: Adatvédelmi incidens nyilvántartás (MINTA)

8. sz. melléklet: Adattovábbítási nyilvántartás (MINTA)

Appendix 1

1. sz. melléklet

Positions with responsibilities related to data control

Adatkezelésért felelős munkakörök

Human resources clerk
Human resources coordinator
Head accountant
Accountant
Financial clerk
Administrator, finance
Budget clerk
Controller
Educational clerk
Administrator, education
Department coordinator
Department assistant
IT staff
CEU ID card official

Humán Erőforrás előadó
Humán Erőforrás koordinátor
Főkönyvelő
Könyvelő
Pénzügyi előadó
Pénzügyi ügyintéző
Költségvetési előadó
Kontroller
Tanulmányi előadó
Tanulmányi ügyintéző
Tanszéki koordinátor
Tanszéki asszisztens
Számítástechnikai munkatárs
ID kártya ügyintéző

As far as paper-based documents are concerned, the Internal Data Protection Officer shall be **Irisz Szél**, in-house legal counsel. E-mail address: szeli@ceu.edu.

As far as electronic documents are concerned, the Internal Data Protection Officer shall be **Szilárd Bedecs**, IT Director. E-mail address: bedecssz@ceu.edu

A papír alapú dokumentumok esetében a belső adatvédelmi felelős **Szél Irisz**, jogtanácsos. E-mail címe: szeli@ceu.edu.

Az elektronikus dokumentumok esetében a belső adatvédelmi felelős: **Bedecs Szilárd**, IT Igazgató. E-mail címe: bedecssz@ceu.edu

Appendix 2

Personal and sensitive data kept and processed by higher education institutions

I. Data of Employees

(1) Data kept pursuant to the NHEA:

a) name, gender, name at birth, place and date of birth, mother's name, citizenship, personal identity number;

b) permanent address, residence and contact address;

c) data referring to employment, public employee status and agency relationship:

ca) name of the employee – or employees – indicating the name of the employer with which the person has established employment relationship,

cb) schooling, professional qualifications, command of foreign languages, scientific degree;

cc) length of service, length of service that can be taken into consideration when calculating the length of public employee service, data referring to position in the hierarchy,

cd) decorations, prizes and other honors and titles,

ce) scope of work, managerial mandate, assignments that lie outside one's scope of work, additional legal relationship related to work, penal sanctions, obligation to pay a fine, obligation to pay damages,

cf) working hours, overtime, payment for work and other remuneration, any sums that have to be subtracted from the pay and the beneficiary of such sums,

cg) annual paid leave, length of leave already used,

ch) sums of money already paid to the employee and the titles of payment,

ci) benefits granted to the employee and their titles,

cj) debts of the employee to the employer and their titles,

2. sz. melléklet

A felsőoktatási intézményekben nyilvántartott és kezelt személyes és különleges adatok

I. Az alkalmazottak adatai

(1) Az Nftv.alapján nyilvántartott adatok:

a) név, nem, születési név, születési hely és idő, anyja neve, állampolgárság, azonosító szám;

b) lakóhely, tartózkodási hely, értesítési cím;

c) munkaviszonyra, közalkalmazotti jogviszonyra, megbízási jogviszonyra vonatkozó adatok:

ca) a munkáltató – több esetén valamennyi munkáltató – megnevezése, megjelölve, hogy mely munkáltatóval létesített foglalkoztatásra irányuló további jogviszonyt,

cb) végzettségi szint, szakképzettség, szakképesítés, idegennyelv-tudás, tudományos fokozat,

cc) munkában töltött idő, közalkalmazotti jogviszonyba beszámítható idő, besorolással kapcsolatos adatok,

cd) kitüntetések, díjak és más elismerések, címek,

ce) munkakör, vezetői megbízás, munkakörbe nem tartozó feladatra történő megbízás, munkavégzésre irányuló további jogviszony, fegyelmi büntetés, kártérítésre kötelezés,

cf) munkavégzés ideje, túlmunka ideje, munkabér, illetmény, továbbá az azokat terhelő tartozás és annak jogosultja,

cg) szabadság, kiadott szabadság,

ch) az alkalmazott részére történő kifizetések és azok jogcímei,

ci) az alkalmazott részére adott juttatások és azok jogcímei,

cj) az alkalmazott munkáltatóval szemben fennálló tartozásai és azok jogcímei,

ck) activity as a researcher, scientific work, creative, artistic activity and its results, data about participation in doctoral training and doctoral procedure in the capacity as instructor or researcher,

cl) The instructor's written statement on which higher education institution may count him in when that institution's conditions of operation are examined for the purpose of applying for subsidies from the state budget,

cm) data proving the fulfilment of requirements specified in Section 25 (4) of the NHEA for fixed term employment established by the higher education institution as an employer related to the president or a member of the financial board,

d) student feedback about the work of the instructor,

e) results of the habilitation procedure,

f) data that help identify the documents that verify the above data.

(2) Additional data may be kept in registers only with the data subject's consent.

II. Data of Students

(1) Data kept in registers pursuant to the NHEA:

a) data related to admission:

aa) the applicant's name, gender, name at birth, mother's name, place and date of birth, citizenship, address, residence, contact address and phone number; if the applicant is not a Hungarian citizen: the status of his residence in Hungary, the name and reference number of the document that certifies the status of his residence in Hungary; as regulated by a separate rule of law: in the case of persons with the right of free movement and residence, the type and reference number of the residence permit;

ab) data about the secondary school-leaving examination,

ac) data about the secondary school,

ck) kutatói tevékenység, tudományos munka, művészeti alkotói tevékenység, azok eredményei, a doktori képzésben és doktori fokozatszerzési eljárásban oktatói, kutatói minőségben történő részvételre vonatkozó adatok,

cl) Az oktató írásban adott nyilatkozata arról, hogy melyik az a felsőoktatási intézmény, amelyiknél az intézmény működési feltételei meglétének mérlegelése során, illetve a felsőoktatási intézmény költségvetési támogatásának megállapításánál figyelembe lehet őt venni,

cm) a felsőoktatási intézmény mint megbízó által megbízási jogviszonyban történő foglalkoztatás - a gazdasági tanács elnöke és tagja - esetén az Nftv. 25. § (4) bekezdésében előírt feltétel igazolására vonatkozó adatok;

d) az oktatói munka hallgatói véleményezésének eredményei,

e) habilitációs eljárás eredménye,

f) az adatokat igazoló okiratok azonosítására szolgáló adatok

(2) A többi adat az érintett hozzájárulásával tartható nyilván.

II. A hallgatók adatai

(1) Az Nftv. alapján nyilvántartott adatok:

a) felvétellel összefüggő adatok:

aa) a jelentkező neve, neme, születési neve, anyja neve, születési helye és ideje, állampolgársága, lakóhelye, tartózkodási helye, értesítési címe és telefonszáma, nem magyar állampolgár esetén Magyarország területén való tartózkodás jogcíme és a tartózkodásra jogosító okirat – külön törvény szerint a szabad mozgás és tartózkodás jogával rendelkező személyek esetén a tartózkodási jogot igazoló okmány - megnevezése, száma,

ab) az érettségi vizsga adatai,

ac) a középiskola adatai,

- ad) data required for a decision on the application to win admission to the University,
- ae) data pertaining to the admission procedure, admission ID No,
- af) the ID No. of the declaration determined in Section 48/D (2) of the NHEA,
- b) data related to student status (doctoral nominee):
- ba) the student's name, gender, name at birth, mother's name, place and date of birth, citizenship, address and phone number of permanent address and residence; contact address and phone number, e-mail address, in case the applicant is not a Hungarian citizen: the status of his residence in Hungary, the name and reference number of the document that certifies the status of his residence in Hungary; as regulated by law: in the case of persons with the right of free movement and residence, the type and reference number of the residence permit;
- bb) date and circumstances of the commencement and termination of student status (doctoral nominee, visiting student), name of the training program the student attends, the form of sponsorship, the work schedule of that program, the expected end date of the course, evaluation of the academic achievements of the student, examination data, semesters commenced, the period of time when the student received support, period of time when the student status is suspended,
- bc) place and date of higher education study tours outside Hungary,
- bd) credits accrued and validated, validated studies,
- be) benefits that the student has received, data required to make a decision on entitlement to benefits (welfare status, data about the parents, data about the student's obligations)
- bf) data about the student's paid working activity,
- bg) data about disciplinary action and damages claims against the student,
- ad) a felvételi kérelem elbírálásához szükséges adatok,
- ae) a felvételi eljárás adatai, a felvételi azonosító;
- af) az Nftv. 48/D. § (2) bekezdése szerinti nyilatkozat azonosító száma;
- b) a hallgatói (doktorjelölti) jogviszonnal összefüggő adatok:
- ba) a hallgató neve, neme, születési neve, anyja neve, születési helye és ideje, állampolgársága, bejelentett lakóhelyének, tartózkodási helyének címe, értesítési címe és telefonszáma, elektronikus levélcíme, nem magyar állampolgár esetén a Magyarország területén való tartózkodás jogcíme és a tartózkodásra jogosító okirat – külön törvény szerint a szabad mozgás és tartózkodás jogával rendelkező személyek esetén a tartózkodási jogot igazoló okmány - megnevezése, száma;
- bb) a hallgatói (doktorjelölti, vendéghallgatói) jogviszonya típusa, keletkezésének és megszűnésének időpontja és módja, a hallgató által folytatott képzés megnevezése, a képzés költségviselési formája és munkarendje, a képzés befejezésének várható időpontja, a hallgató tanulmányainak értékelése, vizsgaadatok, megkezdett félévek, igénybe vett támogatási idő, a hallgatói jogviszony szünetelésének ideje,
- bc) a külföldi felsőoktatási résztanulmányok helye, ideje,
- bd) a képzés során megszerzett és elismert kreditek, beszámított tanulmányok,
- be) a hallgatói juttatások adatai, a juttatásokra való jogosultság elbírálásához szükséges adatok (szociális helyzet, szülők adatai, tartásra vonatkozó adatok),
- bf) a hallgatói munkavégzés adatai,
- bg) a hallgatói fegyelmi és kártérítési ügyekkel kapcsolatos adatok,

- bh) data required to make a decision about benefits to which persons with disabilities are entitled,
- bi) data about the student's accidents,
- bj) the serial number of the university ID card (CEU ID card) of the student, the ID number of the student's registration card,
- bk) the student's ID number, and social security ID code,
- bl) data pertaining to completion of practical courses, pre-degree certificate, final examination (doctoral defence), language examination, and data pertaining to the diploma, diploma supplement,
- bm) data related to the fulfillment of rights and duties pursuant to the student status;
- c) data related to student tracking;
- d) the student's tax identification number;
- e) data that help identify the documents that verify the above data,
- f) data pertaining to the fees paid by the student, data of any related installment payment discount, postponement, exemption;
- g) for those receiving student support, child care support, child care allowance, regular child protection benefit, accommodation grant the data thereof,
- h) data pertaining to the grant – established in a Governmental Decree according to Article 85 (1) and (2) of the NHEA - provided for supporting the education of the student, with respect to the student status of the student,
- i) data pertaining to measuring student competency, to the results thereof.
- (2) Additional data may be kept in registers only with the data subject's consent.
- bh) a fogyatékossgal élőket megillető különleges bánásmód elbírálásához szükséges adatok,
- bi) a hallgatói balesetre vonatkozó adatok,
- bj) a hallgató diákigazolványának sorszáma, a törzslap azonosító száma,
- bk) a hallgató azonosító száma, társadalombiztosítási azonosító jele,
- bl) a szakmai gyakorlat teljesítésére, az abszolutóriumra, a záróvizsgára (doktori védésre), a nyelvvizsgára, valamint az oklevélre, oklevélmellékletre vonatkozó adatok,
- bm) a hallgatói jogviszonyból adódó jogok és kötelezettségek teljesítéséhez szükséges adatok;
- c) a hallgatói pályakövetéssel kapcsolatos adatok;
- d) a hallgató adóazonosító jele;
- e) az adatokat igazoló okiratok azonosítására szolgáló adatok,
- f) a hallgató által fizetett díjak és térítések - a kötelezettséghez kapcsolódó részletfizetési kedvezmény, halasztás, mentesség - adatai;
- g) hallgatói támogatásban gyermekgondozást segítő ellátásban, gyermekgondozási díjban, rendszeres gyermekvédelmi támogatásban, lakhatási támogatásban részesülés esetén e támogatások adatai;
- h) a hallgató tanulmányai támogatása érdekében, a hallgató jogviszonyára tekintettel folyósított – az Nftv. 85. § (1) és (2) bekezdésében foglaltak szerint a Kormány által rendelettel alapított - ösztöndíj adatai;
- i) a hallgatói kompetenciamérésre, annak eredményére vonatkozó adatok.
- (2) A többi adat az érintett hozzájárulásával tartható nyilván.

Appendix 3

FORM

**on the University's internal data
protection register**

1. Data control

**1.1 Name of the data controlling
official:**

1.2 Name of the organizational unit

1.3 Type of data control

1.4 Purpose of data control

1.5 Legal basis:

**1.5.1 The legal provision cited or
other legal ground**

1.5.2 Title of the relevant law

1.6 Location of actual data control

2. Source of data

2.1 Type of data:

2.2 Indication of the source of data:

**2.3 Legal justification for obtaining
the data:**

**2.3.1 The legal provision cited or other legal
ground**

3. sz. melléklet

ADATLAP

**Az Egyetem belső adatvédelmi
nyilvántartásához**

1. Adatkezelés

**1.1 Az adatkezelésért felelős személy
megnevezése:**

1.2 Belső szervezeti egység

1.3 Az adatkezelés megnevezése

1.4 Az adatkezelés célja

1.5 Jogalapja:

**1.5.1 Jogszabályhely vagy más
jogalap**

1.5.2 Jogszabály címe

1.6 Tényleges adatkezelés helye

2. Az adatok forrása

2.1 Adatfajta megnevezése:

2.2 Adatforrás megnevezése:

2.3 Adatfelvétel jogalapja:

2.3.1 Jogszabályhely vagy más jogalap

2.3.2 Title of the relevant law

2.3.2 Jogszabály címe

2.4 Method of obtaining the data:

2.4 Adatfelvétel módja:

2.5 Deadline for the deletion of the data:

2.5 Az adat törlési határideje:

3. Data subject:

3. Adat érintettje:

3.1 Data subject's name:

3.1 Érintett neve:

3.2 Data subject's place and date of birth:

3.2 Érintett születési helye, ideje:

3.3 Name of the mother of the data subject:

3.3 Érintett anyja neve:

Appendix 4

4. sz. melléklet

Summary of the legal provisions on the consequences of violating the rules of personal data control

A személyes adatok kezelésére vonatkozó szabályok megsértésére vonatkozó jogkövetkezmények (a vonatkozó jogszabályi előírások) összefoglalása

(1) Any person who, in violation of the statutory provisions governing the protection and control of personal data:

a) is engaged in the unauthorized and inappropriate controlling of personal data; or
b) fails to take measures to ensure the security of data, or profit making purposes or by causing considerable injury of interest is guilty of a misdemeanor under Article 219 of Act C of 2012 on the Criminal Code.

(2) A person whose privacy rights are violated may, depending on the circumstances of the case, seek a civil law remedy under Article 2:51, 2:52 and 2:53 of the Hungarian Civil Code.

(1) Aki a személyes adatok védelméről vagy kezeléséről szóló törvényi rendelkezések megszegésével haszonszerzési célból vagy jelentős érdeksérelmet okozva

a) jogosulatlanul vagy a céltól eltérően személyes adatot kezel, vagy
b) az adatok biztonságát szolgáló intézkedést elmulasztja, a Büntető Törvénykönyvről szóló 2012. évi C. törvény 219. §-ában meghatározott, „Személyes adattal visszaélés” vétséget követi el.

(2) Akit személyiségi jogában megsértenek, az eset körülményeihez képest a Ptk. 2:51. §-ában, 2:52. §-ában és 2:53. §-ában meghatározott polgári jogi igényeket támaszthatja.

Appendix 5

Information on legal remedies

Remedies ensured by the Data Protection Act

15. § (1) Upon the data subject's request the data controller shall provide information concerning the data relating to him/her, including those processed by a data processor hired by the data controller or by others based on its instructions, the sources from where they were obtained, the purpose, grounds and duration of processing, the name and address of the data processor and on its activities relating to data processing, the circumstances of the privacy incident, its effects and the measures taken for the elimination thereof, and - if the personal data of the data subject is made available to others - the legal basis and the recipients.

(4) The data controller must comply with requests for information without any delay, and provide the information requested in an intelligible form, in writing at the data subject's request, within not more than twenty five days.

18. § (2) If the data controller refuses to comply with the data subject's request for rectification, blocking or erasure, the factual or legal reasons on which the decision for refusing the request for rectification, blocking or erasure is based shall be communicated in writing or – with the consent of the data subject - electronically within twenty five days of receipt of the request. Where rectification, blocking or erasure is refused, the data controller shall inform the data subject of the possibilities for seeking judicial remedy or lodging a complaint with the Authority.

21. § (1) The data subject shall have the right to object to the controlling of data relating to him/her:

a) if data control or disclosure is carried out solely for the purpose of discharging the controller's legal obligation or for enforcing

5. sz. melléklet

Tájékoztató a jogorvoslati lehetőségekről

Az Info. tv. által biztosított jogorvoslati lehetőségek

15. § (1) Az érintett kérelmére az adatkezelő tájékoztatást ad az érintett általa kezelt, illetve az általa vagy rendelkezése szerint megbízott adatfeldolgozó által feldolgozott adatairól, azok forrásáról, az adatkezelés céljáról, jogalapjáról, időtartamáról, az adatfeldolgozó nevééről, címéről és az adatkezeléssel összefüggő tevékenységéről, az adatvédelmi incidens körülményeiről, hatásairól és az elhárítására megtett intézkedésekről, továbbá - az érintett személyes adatainak továbbítása esetén - az adattovábbítás jogalapjáról és címzettjéről.

(4) Az adatkezelő köteles a kérelem benyújtásától számított legrövidebb idő alatt, legfeljebb azonban 25 napon belül, közérthető formában, az érintett erre irányuló kérelmére írásban megadni a tájékoztatást.

18. § (2) Ha az adatkezelő az érintett helyesbítés, zárolás vagy törlés iránti kérelmét nem teljesíti, a kérelem kézhezvételét követő 25 napon belül írásban vagy az érintett hozzájárulásával elektronikus úton közli a helyesbítés, zárolás vagy törlés iránti kérelem elutasításának ténybeli és jogi indokait. A helyesbítés, törlés vagy zárolás iránti kérelem elutasítása esetén az adatkezelő tájékoztatja az érintettet a bírósági jogorvoslat, továbbá a Hatósághoz fordulás lehetőségéről.

21. § (1) Az érintett tiltakozhat személyes adatainak kezelése ellen,

a) ha a személyes adatok kezelése vagy továbbítása kizárólag az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez

the rights and legitimate interests of the controller, the recipient or a third party, unless data control is mandatory;

b) if personal data is used or disclosed for the purposes of direct marketing, public opinion polling or scientific research; and

c) in all other cases prescribed by law.

(2) In the event of objection, the controller shall investigate the cause of objection within the shortest possible time inside a fifteen-day time period, adopt a decision as to merits and shall notify the data subject in writing of its decision.

(3) If, according to the findings of the controller, the data subject's objection is justified, the controller shall terminate all processing operations (including data collection and transmission), block the data involved and notify all recipients to whom any of these data had previously been transferred concerning the objection and the ensuing measures, upon which these recipients shall also take measures regarding the enforcement of the objection.

(4) If the data subject disagrees with the decision taken by the controller under Subsection (2), or if the controller fails to meet the deadline specified in Subsection (2), the data subject shall have the right under Section 22 to bring action in the court of law within thirty days of the date of delivery of the decision or from the last day of the time limit.

22. § (1) In the event of any infringement of his/her rights, the data subject, and in the cases referred to in Section 21, the data recipient may file for court action against the controller. The court shall hear such cases in priority proceedings.

(2) The burden of proof to show compliance with the law lies with the data controller.

vagy az adatkezelő, adatátvevő vagy harmadik személy jogos érdekének érvényesítéséhez szükséges, kivéve kötelező adatkezelés esetén;

b) ha a személyes adat felhasználása vagy továbbítása közvetlen üzletszerzés, közvélemény-kutatás vagy tudományos kutatás céljára történik; valamint

c) törvényben meghatározott egyéb esetben.

(2) Az adatkezelő a tiltakozást a kérelem benyújtásától számított legrövidebb időn belül, de legfeljebb 15 napon belül megvizsgálja, annak megalapozottsága kérdésében döntést hoz, és döntéséről a kérelmezőt írásban tájékoztatja.

(3) Ha az adatkezelő az érintett tiltakozásának megalapozottságát megállapítja, az adatkezelést - beleértve a további adatfelvételt és adattovábbítást is - megszünteti, és az adatokat zárolja, valamint a tiltakozásról, továbbá az annak alapján tett intézkedésekről értesíti mindazokat, akik részére a tiltakozással érintett személyes adatot korábban továbbította, és akik kötelesek intézkedni a tiltakozási jog érvényesítése érdekében.

(4) Ha az érintett az adatkezelőnek a (2) bekezdés alapján meghozott döntésével nem ért egyet, illetve ha az adatkezelő a (2) bekezdés szerinti határidőt elmulasztja, az érintett - a döntés közlésétől, illetve a határidő utolsó napjától számított 30 napon belül - a 22. §-ban meghatározott módon bírósághoz fordulhat.

22. § (1) Az érintett a jogainak megsértése esetén, valamint a 21. §-ban meghatározott esetekben az adatátvevő az adatkezelő ellen bírósághoz fordulhat. A bíróság az ügyben soron kívül jár el.

(2) Azt, hogy az adatkezelés a jogszabályban foglaltaknak megfelel, az adatkezelő köteles bizonyítani.

(3) The action shall be heard by the competent general court. If so requested by the data subject, the action may be brought before the general court in whose jurisdiction the data subject's home address or temporary residence is located.

(4) Any person otherwise lacking legal capacity to be a party to legal proceedings may also be involved in such actions. The Authority may intervene in the action on the data subject's behalf.

(5) When the court's decision is in favor of the plaintiff, the court shall order the controller to provide the information, to rectify, block or erase the data in question, to annul the decision adopted by means of automated data-processing systems, to honor the data subject's objection, or to disclose the data requested by the data recipient referred to in Section 21 of the DPA.

(6) If, in cases under Article 21 of the DPA, the court rejects the request of the data recipient, the data controller shall delete the data of the data subject within 3 days from the notification of the court decision. The data controller shall also delete the data, if the data recipient fails to turn to the court within the deadline determined in Articles 21 (5) and (6) of the DPA.

(7) The court may order publication of its decision, indicating the identification data of the controller as well, where this is deemed necessary for reasons of data protection or in connection with the rights of large numbers of data subjects under protection by the DPA.

23. § (1) Data controllers shall be liable for any damage caused to a data subject as a result of unlawful processing or by any breach of data security requirements.

(2) Where a data controller violates the rights of the data subject relating to personality as a result of unlawful processing or by any

(3) A per elbírálása a törvényszék hatáskörébe tartozik. A per - az érintett választása szerint - az érintett lakóhelye vagy tartózkodási helye szerinti törvényszék előtt is megindítható.

(4) A perben fél lehet az is, akinek egyébként nincs perbeli jogképessége. A perbe a Hatóság az érintett pernyertessége érdekében beavatkozhat.

(5) Ha a bíróság a kérelemnek helyt ad, az adatkezelőt a tájékoztatás megadására, az adat helyesbítésére, zárolására, törlésére, az automatizált adatfeldolgozással hozott döntés megsemmisítésére, az érintett tiltakozási jogának figyelembevételére, illetve az Info tv. 21. §-ban meghatározott adatátvevő által kért adat kiadására kötelezi.

(6) Ha a bíróság az Info tv. 21. §-ban meghatározott esetekben az adatátvevő kérelmét elutasítja, az adatkezelő köteles az érintett személyes adatát az ítélet közlésétől számított 3 napon belül törölni. Az adatkezelő köteles az adatokat akkor is törölni, ha az adatátvevő az Info tv. 21. § (5), illetve (6) bekezdésében meghatározott határidőn belül nem fordul bírósághoz.

(7) A bíróság elrendelheti ítéletének - az adatkezelő azonosító adatainak közzétételével történő - nyilvánosságra hozatalát, ha azt az adatvédelem érdekei és nagyobb számú érintettnek az Info. tv-ben védett jogai megkövetelik.

23. § (1) Ha az adatkezelő az érintett adatainak jogellenes kezelésével vagy az adatbiztonság követelményeinek megszegésével másnak kárt okoz, köteles azt megtéríteni.

(2) Ha az adatkezelő az érintett adatainak jogellenes kezelésével vagy az adatbiztonság követelményeinek megszegésével az érintett

breach of data security requirements, the data subject shall be entitled to demand restitution from the data controller.

(3) The data controller shall also be liable for any damage caused by a data processor acting on its behalf, as well as for any restitution payable to the data subject for any violation by the data processor of his rights relating to personality. The data controller may be exempted from liability for damages or for payment of restitution if he/she proves that the damage was caused by or the violation of the rights of the data subject relating to personality is attributable to reasons beyond his control.

(4) No compensation shall be paid and no restitution may be demanded where the damage was caused by or the violation of rights relating to personality is attributable to intentional or negligent conduct on the part of the data subject.

Legal remedies ensured by Act CXIX of 1995 on the Use of name and Address Information Serving the Purposes of Research and Direct Marketing

20. § (1) Each subject party shall have the right

a) to withhold or prohibit his name and address information included in mailing lists and marketing lists, from being used for direct marketing or other concrete purposes to be established as part of direct marketing, to withhold and prohibit such information from being surrendered to third parties;

b) to request that the use of his personal data in connection with all mailing lists and marketing lists - as well as those for specific purposes - be terminated, including data surrendered to third parties. The data user must notify the subject party of the fulfilment of his request.

személyiségi jogát megsérti, az érintett az adatkezelőtől sérelemdíjat követelhet.

(3) Az érintettel szemben az adatkezelő felel az adatfeldolgozó által okozott kárért és az adatkezelő köteles megfizetni az érintettnek az adatfeldolgozó által okozott személyiségi jogsértés esetén járó sérelemdíjat is. Az adatkezelő mentesül az okozott kárért való felelősség és a sérelemdíj megfizetésének kötelezettsége alól, ha bizonyítja, hogy a kárt vagy az érintett személyiségi jogának sérelmét az adatkezelés körén kívül eső elháríthatatlan ok idézte elő.

(4) Nem kell megtéríteni a kárt és nem követelhető a sérelemdíj annyiban, amennyiben a kár a károsult vagy a személyiségi jog megsértésével okozott jogsérelem az érintett szándékos vagy súlyosan gondatlan magatartásából származott.

A kutatás és a közvetlen üzletszerzés célját szolgáló név- és lakcímadatok kezeléséről szóló 1995. évi CXIX. törvény által biztosított jogorvoslati lehetőségek

20. § (1) Minden érintettnek joga van arra, hogy

a) megtagadja vagy megtiltsa név- és lakcímadatainak a kapcsolatfelvételi, illetve üzletszerzési listán való szerepeltetését, közvetlen üzletszerzési - illetőleg azon belül meghatározott konkrét - célra történő felhasználását, illetőleg harmadik személynek átadását;

b) kérje személyes adatainak az adatkezelő birtokában lévő valamennyi vagy meghatározott célú kapcsolatfelvételi, illetve üzletszerzési listán történő kezelésének megszüntetését, beleértve a harmadik személy részére átadott adatokat is. Az adatkezelő köteles írásban tájékoztatni az érintettet kérésének teljesítéséről.

Appendix 6

6. sz. melléklet

INFORMATION ON DATA PROCESSING (SAMPLE)

ADATVÉDELMI TÁJÉKOZTATÓ (MINTA)

Közép-európai Egyetem and the Central European University, New York (collectively: the “University”) performs personal data management of [...] (hereinafter referred to as the „Data Subject”) during the operation of the [...] database (hereinafter referred to as: „Database”).

A Közép-európai Egyetem és a Central European University, New York (együttesen az „Egyetem”) az [...] adatbázis (a továbbiakban: „Adatbázis”) működtetése során az itt regisztrált [...] (a továbbiakban: „Érintettek”) személyes adatainak kezelését végzi.

The University controls all personal data of the Data Subjects in line with the applicable Hungarian legal provisions, specifically, but not limited to Act CCIV of 2011 on National Higher Education, Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information, Act V of 2013 on the Civil Code as well as in line with its Personal Data Protection Policy.

Az Egyetem az Érintettekkel kapcsolatos személyes adatokat a vonatkozó magyar jogszabályokkal, így különösen, de nem kizárólagosan a nemzeti felsőoktatásról szóló 2011. évi CCIV. törvény, az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény, a Polgári Törvénykönyvről szóló 2013. évi V. törvény, valamint az Egyetem személyes adatok védelméről szóló szabályzatának rendelkezéseivel összhangban kezeli.

Description of the data involved in data control:
[...]

A kezelt adatok köre:
[...]

The duration of data control:
[...]

Az adatkezelés időtartama:
[...]

Purpose of data control:
[...]

Az adatkezelés célja:
[...]

The legal basis of data control:
[...]

Az adatkezelés jogalapja:
[...]

Transmission of data:
[...]

Adattovábbítás:
[...]

The legal basis of data transmission:
[...]

Az adattovábbítás jogalapja:
[...]

Az adatkezelésre jogosult személyek:
[...]

Person entitled to data management:
[...]

7. sz. melléklet
Adatvédelmi incidens nyilvántartás (MINTA)

Sorszám	Az érintett személyes adatok köre	Az adatvédelmi incidenssel érintettek köre	Az adatvédelmi incidenssel érintettek száma	Az adatvédelmi incidens időpontja	Az adatvédelmi incidens körülményei	Az adatvédelmi incidens hatásai	Az adatvédelmi incidens elhárítására tett intézkedések	Az adatkezelést előíró, jogszabályban meghatározott egyéb adatok	Bejegyzés dátuma (év, hó, nap)

Appendix 7
Privacy Incident (SAMPLE)

No.	Range of affected personal data	Persons affected by the privacy incident	No of persons affected by the privacy incident	Date of the privacy incident	Circumstances of the privacy incident	Effects of the privacy incident	Measures taken for eliminating the privacy incident	Other data determined in the law	Date of recording (day, month, year)

8. sz. melléklet
Adattovábbítási nyilvántartás (MINTA)

Sorszám	Az adattovábbítást teljesítő szervezeti egység neve	A személyes adatok továbbításának időpontja	Az adattovábbítás jogalapja	Az adattovábbítás címzettje	Továbbított személyes adatok köre	Egyéb adatok	Bejegyezte (név)	Bejegyzés dátuma (év, hó, nap)	Megjegyzés

Appendix 8
Data Transmission Register (SAMPLE)

No.	Name of the department transmitting data	Date of personal data transmission	Legal basis of data transmission	Addressee of data transmission	Transmitted personal data	Other data	Recorded by	Date of recording (day, month, year)	Notes

Document information	
Type	Policy
Number	P-1611-2
Title	Personal Data Protection Policy
Distribution	Internal
Filename	P-1611-2 Personal Data Protection Policy
Notes	
Related documents	
For final documents	
Approved by:	Senate
Date of approval	November 23, 2016 and May 26, 2017
Enters force	May 29, 2017