

## A HCEMM NONPROFIT KFT. ADATKEZELÉSI ÉS ADATVÉDELMI SZABÁLYZATA

### 1. FEJEZET - ÁLTALÁNOS TÁJÉKOZTATÓ A WEBOLDAL LÁTOGATÓKNAK ÉS ÜGYFELEINKNEK, PARTNEREINKNEK

(1) Jelen Adatkezelési és Adatvédelmi Szabályzat (a továbbiakban: „Szabályzat”) útmutatást nyújtunk Társaságunk adatkezelési és adatvédelmi szabályairól weboldalunk látogatójának, valamint minden személynek, aki a szolgáltatásainkat igénybe veszik, illetve Társaságunkkal szerződéses kapcsolatba lépnek. Fontos számunkra, hogy minden érintett megfelelő technikai-informatikai védelemben érezze magát és az átadott személyes adatait. Ezen kívül kiemelt fontosságú, hogy átlátható módon, egyértelmű tájékoztatást kapjon valamennyi kapcsolódó adatkezelési tevékenységünkéről.

(2) A HCEMM Nonprofit Kft. a személyes adatokat, illetve a közérdekű adatokat az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: „Info tv.”) és a Nemzeti Adatvédelmi és Információszabadság Hatóság elnöke által kiadott állásfoglalásoknak megfelelően kezeli, összhangban a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (Általános Adatvédelmi Rendelet) szóló, az Európai Parlament és a Tanács (EU) 2016/679 Rendeletével (a továbbiakban: „GDPR”).

(3) Jelen Szabályzat célja, hogy a lehető legérthatőbb formában közölje az érintettekkel (akiknek a személyes adatait Társaságunk valamelyik, a lenti részletezett formában kezeli), hogy ki, mire, mikor, hogyan és milyen célból használhatja fel az általuk szolgáltatott adatokat, valamint felvilágosítást nyújtson a jogainkról és adott esetekben a jogorvoslati lehetőségekről is. Cél továbbá, hogy harmonizálja az egyes adatkezelési tevékenységek tekintetében a szervezetünk belső szabályzatainak előírásait a természetes személyek alapvető jogainak és szabadságainak védelme érdekében, valamint biztosítsa a személyes adatok megfelelő kezelését. A jelen Szabályzat megismerésével és betartásával Társaságunk munkatársai, az egyes szervezeti egységek vezetői felkészültté válnak annak érdekében, hogy a természetes személyek adatai kezelését jogosító végezzék, egyúttal, hogy Társaságunk biztosítsa az adatvédelem alkotmányos elveinek, az adatbiztonság követelményeinek érvényesülését, megakadályozza az adatokhoz való jogosulatlan hozzáférést, és azok jogosulatlan megváltoztatását, elvesztését, illetve nyilvánosságra hozatalát.

(4) Az adatkezeléssel érintett a személyes adatainak megadásával elfogadja jelen Szabályzatban foglalt feltételeket.

### DATA PROCESSING AND DATA PROTECTION POLICY OF THE HCEMM NONPROFIT KFT.

#### ARTICLE 1 - GENERAL INFORMATION FOR THE WEBSITE VISITORS, OUR CLIENTS AND PARTNERS

(1) By this present Data Processing and Data Protection Policy (hereinafter referred to as "Policy") we provide guidance on our Company's data management and data protection rules to the visitors of our website and to all those who use our services or enter into a contractual relationship with our Company. It is important for us that all data subjects feel that they and their provided personal data are adequately protected regarding both technical and IT protection. In addition to the aforementioned, it is of paramount importance that you receive clear and unambiguous information about all our related data management activities.

(2) The personal data and data of public interest are handled by HCEMM Non-profit Kft. in accordance with Act CXII of 2011 on Informational Self-Determination and Freedom of Information (hereinafter referred to as "Privacy Act") and the approaches issued by the Chairperson of the National Authority for Data Protection and Freedom, in consonance with regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter referred to as the "GDPR").

(3) The purpose of this Policy is to inform the data subjects (whose personal data is processed by our Company in one of the ways detailed below) in the most comprehensible way possible about who, for what, when, how and for what purpose their provided data may be used, as well as to provide information on their rights and where appropriate, their judicial remedies. It also aims to harmonise the requirements of our organisation's internal rules for each data processing activity in order to protect the fundamental rights and freedoms of natural persons and to ensure the proper processing of personal data. By getting to know and complying with this Policy, the employees of our Company and the heads of individual organisational units will be prepared to process the data of natural persons lawfully, and at the same time to ensure the constitutional principles of data protection and data security requirements, their unauthorised alteration, and loss of disclosure.

(4) By providing personal data, the data subject agrees to the terms and conditions contained in this Policy.



## 2. FEJEZET - AZ ADATKEZELŐ ELÉRHETŐSÉGEI

Név/cégnév: HCEMM Nonprofit Kft.  
Székhely: 6720 Szeged, Dugonics tér 13.  
Levelezési cím: 6723 Szeged, Római körút 21.  
Adószám: 26307383-2-06  
Weboldal megnevezése, címe: [www.hcemm.eu](http://www.hcemm.eu)  
Jelen Szabályzat elérhető:  
[www.hcemm.eu/adatkezeles](http://www.hcemm.eu/adatkezeles)  
E-mail: gdpr@hcemm.eu

(1) A HCEMM Nonprofit Kft., mint adatkezelő, magára nézve kötelezőnek ismeri el jelen Szabályzat, a saját tevékenységével kapcsolatos minden adatkezelés során arra törekszik, hogy az adatkezelési műveletei során minden területen megfeleljen a jelen Szabályzatban, belső szabályzataiban és a hatályos jogszabályokban meghatározott elvárásoknak.

## 3. FEJEZET - ADATFELDOLGOZÓK NEVE ÉS ELÉRHETŐSÉGE

(1) Az adatfeldolgozók neve és elérhetősége a jelen Szabályzat 1. számú mellékletében található.

## 4. FEJEZET - FOGALMAK

4.1 A jelen Szabályzat értelmében:

(1) „**GDPR**” az Európai Parlament és Tanács (EU) 2016/679 számú rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (Általános Adatvédelmi Rendelet);

(2) „**Adatkezelés**” a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés, továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétele útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés;

(3) „**Adatkezelések nyilvántartása**” a GDPR 30. cikk (1) bekezdésében foglalt kötelezettség alapján az adatkezelő által végzett adatkezelési tevékenységekről szóló nyilvántartás, mely tartalmazza az adatkezelőre vonatkozó adatokon túl az adatkezelés megnevezését, az adatkezelés célját, az érintettek kategóriáit, a kezelt személyes adatok kategóriáit, ha lehetséges, a címzetteket akikkel az adatokat közölni fogják, az adatfeldolgozó(k) nevét és elérhetőségeit, továbbá – ha lehetséges – az egyes adatkategóriák törlésére előirányzott határidőt;

(4) „**Adatfeldolgozó**”: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel;

## ARTICLE 2 - CONTACTS OF DATA PROCESSOR

Company name: HCEMM Non-profit Kft.  
Registered seat: 6720 Szeged, Dugonics tér 13.  
Mailing address: 6723 Szeged, Római körút 21.  
Tax number: 26307383-2-06  
Name and address of website: [www.hcemm.eu](http://www.hcemm.eu)  
This Policy is available at:  
[www.hcemm.eu/adatkezeles](http://www.hcemm.eu/adatkezeles)  
E-mail: gdpr@hcemm.eu

(1) HCEMM Non-profit Kft. as data processor, is bound by this Policy. In all data processing related to its own activities it strives to comply with the requirements specified in this Policy, its internal regulations and the applicable legislation in all areas of its data processing operations.

## ARTICLE 3 - NAMES AND CONTACTS OF DATA PROCESSORS

(1) The names and contacts of data processors can be found in Annex 1 to this Policy.

## ARTICLE 4 - DEFINITIONS

4.1 For the purpose of this Policy:

(1) “**GDPR**” means the regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);

(2) “**Data Processing**” means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

(3) “**Record of data processing activities**” means based on Section 1 of Article 30 of the GDPR the record of processing activities maintained by the controller contains - beyond data of the controller - the purposes of the processing, the description of the categories of data subjects, the categories of the processed personal data, where possible the categories of recipients to whom the personal data will be disclosed, the name and contact of processor(s) and, where possible the envisaged time limits for erasure of the different categories of data;

(4) “**Data Processor**” means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;



(5) „**Személyes adat**” azonosított vagy azonosítható természetes személyre (érintett) vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fisiológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható;

(6) „**Különleges adat**” a faji eredetre, a nemzetiségezhez tartozásra, a politikai véleményre vagy párttállásra, a vallásra vagy más világnézeti meggyőződésre, az érdekképviseleti szervezeti tagságra, a szexuális élethez vonatkozó személyes adat, az egészségi állapotra, a kóros szenvedélyre vonatkozó személyes adat, valamint a bűnfügyi személyes adat;

(7) „**Genetikai adat**” egy természetes személy örökölt vagy szerzett genetikai jellemzőre vonatkozó minden olyan személyes adat, amely az adott személy fiziológiájára vagy egészségi állapotára vonatkozó egyedi információt hordoz, és amely elsősorban az említett természetes személyből vett biológiai minta elemzéséből ered;

(8) „**Biometrikus adat**” egy természetes személy testi, fisiológiai vagy viselkedési jellemzőre vonatkozó minden olyan sajátos technikai eljárásokkal nyert személyes adat, amely lehetővé teszi vagy megerősíti a természetes személy egyedi azonosítását, ilyen például az arckép vagy a dactiloszkópiai adat;

(9) „**Egészségügyi adat**” egy természetes személy testi vagy pszichikai egészségi állapotára vonatkozó személyes adat, ideértve a természetes személy számára nyújtott egészségügyi szolgáltatásokra vonatkozó olyan adatot is, amely információt hordoz a természetes személy egészségi állapotáról;

(10) „**Adatkezelő**” az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza; ha az adatkezelés céljait és eszközeit az európai uniós vagy a tagállami jog határozza meg, az adatkezelőt vagy az adatkezelő kijelölésére vonatkozó különös szempontokat az európai uniós vagy a tagállami jog is meghatározhatja;

(11) „**Az érintett hozzájárulása**” az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló és egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez;

(12) „**Adatvédelmi incideens**” a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, meg változtatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi;

(13) „**Címzett**” az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, aki vel vagy amellyel a személyes adatot közlik, függetlenül attól, hogy harmadik fél-e. Azon közhatalmi szervek, amelyek egy egyedi vizsgálat keretében az uniós vagy a tagállami joggal összhangban férhetnek hozzá személyes adatokhoz, nem minősülnek címzettek; az említett adatok e közhatalmi szervek általi kezelése meg kell, hogy felejten az adatkezelés

(5) „**Personal data**” means any information relating to an identified or identifiable natural person („data subject”); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

(6) „**Special data**” means any data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic or health status or sexual orientation;

(7) „**Genetic data**” means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

(8) „**Biometric data**” means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

(9) „**Data concerning health**” means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

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

(11) „**Consent of the data subject**” means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

(12) „**Personal data breach**” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

(13) „**Recipient**” means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not; However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance



céljainak megfelelően az alkalmazandó adatvédelmi szabályoknak;

(14) „**Harmadik fél**” az a természetes vagy jogi személy, közhangalmi szerv, ügynökség vagy bármely egyéb szerv, amely nem azonos az érintettel, az adatkezelővel, az adatfeldolgozóval vagy azokkal a személyekkel, akik az adatkezelő vagy adatfeldolgozó közvetlen irányítása alatt a személyes adatok kezelésére felhatalmazást kaptak;

(15) „**Adatvédelmi Tisztviselő**” a Társaságunk által a GDPR 37. cikk (1) bekezdés a.) pontja alapján kijelölt személy, akinek elérhetőségeit és jogállását jelen Szabályzat tartalmazza;

(16) „**Hatóság**” a Nemzeti Adatvédelmi és Információbiztonsági Hatóság (a továbbiakban: „NAIH”);

(17) „**Európai Molekuláris Biológiai Laboratórium**” (a továbbiakban: EMBL) elettudományokkal foglalkozó európai államközi kutatási szervezet, amely kutatási teljesítménye a genetikával és molekuláris biológiával foglalkozó európai intézetek között az első. A kiváló színvonalú molekuláris és sejtbiológiai facilitásokon túl stratégiaileg kiemelkedően fontos infrastruktúrákat működtet a bioinformatika és a szerkezetbiológia területén. Vezető szerepet játszik az európai élettani kutatások integrálásában, hét uniós orvosbiológiai kutatási infrastruktúra-projektben vesz részt;

(18) „**Horizon 2020 keretprogram**” kiválósági alapon, nemzetközi versenyben, közvetlenül Brüsszelből elnyerhető pályázati forrásokat jelent: a pályázatok brüsszeli elbírálásánál döntő szempont a kiválóság, a magas szakmai szintű és jól menedzselt konzorcium, illetve az uniós szinten is mérhető hatás, vagyis a rendelkezésre álló pénzügyi keretből mindegyik tagállam annyit hasznosít, amennyit az uniós versenyben elnyerni képesek a projektjei. A Horizont 2020 keretprogram a kontinens globális versenyképességének növelését célzó Európa 2020 stratégia „Innovatív Unió” elnevezésű kiemelt kezdeményezésének egyik alappillére, az Unió kutatás-fejlesztési és innovációs szakpolitikájának legfőbb eszköze;

(19) „**Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal**” (a továbbiakban „NKFIH”) célja a tudományos kutatásról, fejlesztésről és innovációról szóló 2014. évi LXXVI. törvény (a továbbiakban: „KFI tv.”) alapján, hogy kialakítsa a hazai kutatás-fejlesztés és innováció (a továbbiakban „KFI”) kormányzati koordinációjának és kiszámítható finanszírozásának stabil intézményi rendszerét, biztosítva a rendelkezésre álló források hatékony, átlátható és értékteremtő felhasználását. Az NKFIH küldetése, hogy kialakítsa a kutatásfinanszírozás koordinált, kiszámítható és fenntartható ösztönzőrendszerét, amelyben a kiváló tudományos kutatások támogatásával és az innováció ösztönzésével Magyarország ne csak szabályszerűen, hanem célszerűen használja fel a KFI célú forrásokat, erősítse hazánk globális versenyképességét, és minél eredményesebb kapcsolódjon be az Európai Kutatási Térségbe. Az NKFIH célkitűzése a nemzeti innovációs rendszer megerősítése, a tudományos központok, vállalatok és vállalkozások dinamikus együttműködésének ösztönzése, a vonzó innovációs környezet kialakítása. Az NKFIH készíti elő hazánk tudományos kutatási, fejlesztési és innovációs stratégiáját, kezeli a Nemzeti Kutatási, Fejlesztési és Innovációs Alap forrásait, képviseli Magyarország Kormányát és a magyar KFI közösséget a nemzetközi és európai KFI szervezetekben.

with the applicable data protection rules according to the purposes of the processing;

(14) “**Third party**” means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;

(15) “**Data Protection Officer**” is the person designated by our Company based on of Section 1 (a) of Article 37 of Regulation (EU) 2016/679 of the European Parliament and of the Council, whose contact and position are contained in this Policy;

(16) “**Authority**” means the Hungarian National Authority for Data Protection and Freedom of Information;

(17) “**European Molecular Biology Laboratory**” (hereinafter referred to as “EMBL”) an intergovernmental organisation specialising in research in the life sciences. Its research performance is the first among European institutes specialising in genetics and molecular biology. In addition to the high-quality molecular and cell biology facilities, it also operates strategically important infrastructures in bioinformatics and structural biology. It is a leader in the integration of European physiological research and is involved in seven EU biomedical research infrastructure projects;

(18) “**Horizon 2020 framework programme**” is the source of funding that can be obtained, in an international competition, directly from Brussels on the basis of excellence. Excellence, a highly professional and well-managed consortium, and a measurable impact at EU level are crucial for the evaluation of proposals in Brussels, such that each Member State can use as much of the available financial framework as can be won by its projects an EU competition. The Horizon 2020 framework programme is one of the cornerstones of the Europe 2020 flagship initiative “Innovation Union” to increase the continent’s global competitiveness, and it is also a key instrument of the EU’s research and development and innovation policy;

(19) “**National Research, Development and Innovation Office’s**” (hereinafter referred to as “NRDIO”) purpose is based on Act LXXVI of 2014 on Scientific Research, Development and Innovation (hereinafter referred to as “KFI tv.”), is to establish a stable institutional system of governmental coordination and predictable financing of domestic research and development and innovation (hereinafter referred to as “RDI”); ensuring efficient, transparent and value-adding use of the available resources. The mission of the NRDIO is to create a coordinated, predictable and sustainable incentive system for research funding, in which, by supporting excellent scientific research and by encouraging innovation, Hungary uses RDI resources not only lawfully but also expediently, strengthens its global competitiveness and enhances its participation in the European Research Area. The objectives of the NRDIO are to strengthen the national innovation system, to encourage dynamic cooperation between research centres, companies and enterprises, and to create an attractive innovation environment. The NRDIO prepares the scientific research, development and innovation strategy of Hungary, manages the resources of the National Research, Development and Innovation Fund, and represents the Government of Hungary and the Hungarian RDI community in international and European RDI organizations.



4.2 Társaságunk, mint Adatkezelő a személyes adatnak minősülő adatkezelése során az alábbi alapelveket követi:

- (1) a személyes adatokat jogosrőben és tisztességesen, valamint az érintettek számára is átláthatóan kezeljük;
- (2) a személyes adatokat csak meghatározott, egyértelmű és jogosről célból gyűjtjük, és azokat nem kezeljük össze nem egyeztethető módon;
- (3) az az általunk gyűjtött és kezelt személyes adatok az adatkezelés céljai szempontjából megfelelők és relevánsak, valamint csak a szükségesre korlátozódnak;
- (4) társaságunk minden ésszerű intézkedést megtesz annak érdekében, hogy az általunk kezelt adatok pontosak és szükség esetén naprakész legyenek, a pontatlan személyes adatokat haladéktalanul töröljük vagy helyesbítjük;
- (5) a személyes adatokat olyan formában tároljuk, hogy az érintettek csak a személyes adatok kezelése céljainkat eléréséhez szükséges ideig legyenek azonosíthatóak;
- (6) megfelelő technikai és szervezési intézkedések alkalmazásával biztosítjuk a személyes adatok megfelelő biztonságát az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szemben.

#### 4.3 A személyes adatok különleges fajtáinak kezelése

(1) Társaságunknál a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a természetes személyek egyedi azonosítását célzó genetikai és biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok kezelése tilos, kivéve, ha:

- a. az érintett kifejezett hozzájárulását adta az említett személyes adatok egy vagy több konkrét célból történő kezeléséhez, kivéve, ha jogszabály úgy rendelkezik, hogy a tilalom nem oldható fel az érintett hozzájárulásával;
- b. az adatkezelés a Társaságunknak vagy az érintettnek a foglalkoztatást, valamint a szociális biztonságot és szociális védelmet szabályozó jogi előfrásokból fakadó kötelezettségei teljesítése és konkrét jogai gyakorlása érdekében szükséges;
- c. az adatkezelés az érintett vagy más természetes személy létfontosságú érdekeinek védelméhez szükséges, ha az érintett fizikai vagy jogi cselekvőképtelensége folytán nem képes a hozzájárulását megadni;
- d. az adatkezelés olyan személyes adatokra vonatkozik, amelyeket az érintett kifejezetten nyilvánosságra hozott;
- e. az adatkezelés jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez szükséges (GDPR 9. cikk).

4.2 As controller, our Company abides by the following principles relating to processing of personal data:

- (1) personal data shall be processed lawfully and in a transparent manner in relation to the data subject;
  - (2) personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
  - (3) personal data collected by us shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
  - (4) our Company takes every reasonable step to ensure that the data collected by us shall be accurate and, where necessary, kept up to date; and to ensure that personal data that are inaccurate, with regard to the purposes for which they are processed, are erased or rectified without delay;
  - (5) personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
  - (6) personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
- #### 4.3 Processing special categories of personal data
- (1) At our Company, processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited, unless:
    - a. the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition may not be lifted by the data subject;
    - b. processing is necessary for the purposes of carrying out the obligations and exercising specific rights of our Company or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
    - c. processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
    - d. processing relates to personal data which are manifestly made public by the data subject;
    - e. processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity (Article 9 of the GDPR).



## 5. FEJEZET- ELEKTRONIKUS MEGFIGYELŐRENDSZER (KAMERÁS RENDSZER) ÜZEMELTETÉSE

(1) Társaságunk telephelyénél egy, a Római körút Irodaházban (6723 Szeged, Római krt. 21.) található, 255 m<sup>2</sup>-es bérlelmény szolgál. Az Irodaház üzemeltetését, beleértve a felszerelt kamerák szakszerű üzemeltetését a Római körút Irodaház Kft. végzi, aki a külön szabályzatban meghatározott számú és típusú kamerát helyezett el az épület különböző részein, beleértve a gépkocsi parkolót, az épület bejáratát és a belső területet is.

(2) Az adatkezelés célját és jogalapját egyaránt a Római körút Irodaház Kft. határozza meg, amit a kamerás megfigyelésre vonatkozó szabályzatokban rögzítenek. Az irodaházban felszerelt kamerarendszer üzemeltetésére vonatkozó Szabályzat és a kamerák elhelyezésének tervrajza külön, önálló dokumentumban találhatók.

## 6. FEJEZET - BELÉPTETŐ RENDSZER ÜZEMELTETÉSE AZ IRODÁK FIZIKAI VÉDELME ÉS AZ INFORMATIKAI RENDSZEREK VÉDELME ÉRDEKÉBEN

6.1 A munkatársaink és a velük együtt érkező vendégek irodába történő belépéseinak ellenőrzése

(1) Társaságunk több aktív adatbiztonsági intézkedéssel törekszik megakadályozni, hogy jogosulatlan személyek hozzáférjenek az informatikai rendszerekhez, amelyekben munkatársaink, illetve az üzleti partnereink személyes adatainak feldolgozása történik („Adatkezelő Rendszerek”), ennek érdekében a kamerás megfigyelőrendszer mellett beléptető rendszert is alkalmazunk.

(2) A Házirendben rögzített szabályok célja az Irodaházban folyó munka professzionális színvonalának fenntartása, biztonságos üzemeltetése és környezetének megőrzése. A Házirend az Irodaház főépületében irodát Bérlők, azok alkalmazottai, valamint vendégei, látogatói által az Irodaház területén betartandó szabályokat foglalja össze. A Házirend kiadásáért, frissítéséért a Római körút Irodaház Kft. felel.

(3) minden olyan adatvédelmi és adatbiztonsági jellegű esemény bekövetkezése, vagy annak kockázata esetén, mely a HCEMM Nonprofit Kft-t érinti, a Római körút Irodaház Kft. megkeresi a HCEMM Nonprofit Kft. Adatvédelmi Tisztviselőjét és / vagy Jogi Igazgatóját.

6.2 Adattovábbítás ellenőrzése

(1) Az adattovábbításra, mint adatkezelési műveletre vonatkozó szabályokat a jelen Szabályzat 8. fejezete, azaz az „Adattovábbításra vonatkozó szabályok, adatkezelési műveletek nyilvántartása” és az Internet Biztonsági Szabályzat (továbbiakban: IBSZ) tartalmazza.

(2) Társaságunk az IBSZ-ben részletesen kifejtett módon és eszközökkel biztosítja, hogy az elektronikus rendszeren történő adattovábbítás során, személyes adatot ne lehessen jogosulatlanul olvasni, másolni, megváltoztatni, vagy eltávolítani, vagy ugyanezt megtenni az adathordozókon történő másolás, tárolás, továbbítás során.

(3) Ennek érdekében Társaságunk különféle titkosítási módszereket alkalmaz, amiket az IBSZ-ben rögzítünk.

## ARTICLE 5 - OPERATION OF ELECTRONIC MONITORING (CAMERA) SYSTEM

(1) Our Company is seated at a 255 m<sup>2</sup> rental property located in the Római körút Office Building (6723 Szeged, Római krt. 21.). The operation of the Office Building, including the professional-technical operation of the equipped cameras, is performed by Római körút Irodaház Kft, that placed a number and type of cameras - specified in a separate regulation - in different parts of the building, including the car park, the building entrance and the interior area.

(2) Both the purpose and the legal basis of data processing are determined by Római körút Irodaház Kft. and set out in the regulations on camera surveillance. The Regulation for the operation of the camera system installed in the office building and the plan for the placement of the cameras can be found in a separate, independent document.

## ARTICLE 6 - OPERATION OF THE ACCESS SYSTEM FOR THE PHYSICAL PROTECTION OF THE OFFICES AND THE PROTECTION OF IT SYSTEMS

6.1 Checking of our staff and their guests entering the office

(1) Our Company takes several active data security measures to prevent unauthorized persons from accessing the IT systems in which the personal data of our employees and business partners are processed ("Data Processing Systems"). For this purpose, we also use an access control system in addition to the camera surveillance system.

(2) The purpose of the rules specified in the House Rules is to maintain the professional standard of the work carried out in the Office Building, to operate it safely and to preserve its environment. The House Rules summarise the rules to be observed by the Tenants of the main Office Building, as well as by their guests and visitors. Római körút Irodaház Kft. is responsible for issuing and updating the House Rules.

(3) In the event of the occurrence or risk of occurrence of any data protection and data security events affecting HCEMM Non-profit Kft., Római körút Irodaház Kft. will contact the Data Protection Officer and / or the Legal Director of HCEMM Non-profit Kft.

6.2 Data transfer control

(1) The rules for data transfer as a data processing operation are contained in Chapter 8 of this Policy, i.e. "Record of rules for data transfer and of data processing operations", and the Internet Security Policy (hereinafter referred to as "ISP").

(2) In the manner and by the means explained in detail in the ISP, our Company ensures that, without authorisation, personal data cannot be read, copied, changed or removed during the data transfer on the electronic system, neither during the copying, storage or transfer via data carriers.

(3) In order to ensure this, our Company uses various encryption methods, which are recorded in the ISP.



(4) Az adattárolás ellenőrzése kapcsán Társaságunk megakadályozza, hogy arra jogosulatlan vagy illetéktelen személyek a személyes adatokhoz hozzáférjenek, de a hozzáférés és a hozzáférésre jogosultak ellenőrzésével ugyancsak megakadályozzuk a tárolt személyes adatok jogosulatlan megtekintését, módosítását, vagy törlését (tárolás ellenőrzése).

(5) A dokumentáció ellenőrzés során Társaságunk biztosítja, hogy képesek legyünk felülvizsgálni az adatkezelő rendszerek összes lényeges feldolgozási lépések dokumentálását, és nyomon követni a személyes adatok feldolgozásnak egyes lépései.

## **7. FEJEZET - AZ ADATKEZELÉS ÉS ADATKEZELÉSI MŰVELETEK, ADATVÉDELMI OKTATÁS**

(1) A Társaságunk által kezelt személyes adatok, az adatkezeléssel érintettek köre, a Társaságunk által végzett adatkezelési műveletek, az adatkezelés időtartama, jogalapja és a kapcsolódó szempontok megjelölését a jelen Szabályzat 23. számú melléklete tartalmazza.

(2) A Társaságunknál megvalósuló egyes adatkezelési folyamatok részletes leírását, a Társaságunk adattérképét, a jelen Szabályzat 21. számú, nem nyilvános melléklete tartalmazza.

(3) Ez utóbbi adatkezelési műveletekről az érintett kérésére esetén, az ő adatai vonatkozásában Társaságunk kész egy tájékoztató kivonatot kiadni.

(4) Társaságunk kizárálag az adatfeldolgozóinkkal kötött megállapodás alapján, az abban foglalt mértékben jogosult az általa kezelt személyes adatok átadására.

### **7.1 Ellenőrzés, belső auditok**

(1) Az adatkezelést végző egyes osztályok felelős vezetői folyamatosan ellenőrzik az adatvédelemmel kapcsolatos előírások, így különösen a jelen Szabályzat és a kapcsolódó dokumentumok rendelkezéseinek betartását. Az Adatvédelmi Tisztviselő a Jogi Igazgatóval együttműködve az ellenőrzést megelőzően megadja a területi vezetők számára a megfelelő szakmai segítséget, illetve azokat a súlypontokat, amelyek alapján azok az ellenőrzést elvégzik.

(2) A felelős személyek listája a jelen Szabályzat 26. számú mellékletében található.

(3) Az egyes adatkezelések ellenőrzésére szükség szerint kerül sor, de legalább évente egy alkalommal kell elvégezni.

(4) Az ellenőrzés tapasztalatairól az Adatvédelmi Tisztviselő írásban tájékoztatja az ügyvezetőt.

(5) Az Adatvédelmi Tisztviselő tájékoztatása elkészítését megelőzően konzultál a Jogi Igazgató és az egyes osztályok vezetőjével és javaslatot ad az ügyvezető részére a szükséges intézkedések megtételére.

(6) Az ellenőrzés során szükségessé vált intézkedések végrehajtásáért az ügyvezető felelős.

(4) In connection with the control of data storage, our Company prevents unauthorised or unwarranted persons from accessing personal data. By controlling access and those who are entitled to access, we also prevent unauthorised viewing, modification or deletion of stored personal data (storage control).

(5) During the review of documentation, our Company ensures that we are able to review the documentation of all relevant processing steps of the data processing systems and to monitor the individual steps of the processing of personal data.

## **ARTICLE 7 - DATA PROCESSING AND DATA PROCESSING OPERATIONS, DATA PROTECTION TRAINING**

(1) The personal data managed by our Company, the data processing subjects, the data processing operations performed by our Company, the duration of the data processing, its legal basis and the related aspects are marked in Appendix no. 23 of this Policy.

(2) The detailed description of each data processing process implemented by our Company, and the data map of our Company are included in the non-public Appendix no. 21 of this Policy.

(3) At the request of the data subject, our Company is ready to issue an information extract on their data processing operation.

(4) Our Company is entitled to transfer personal data processed by it only on the basis of the agreement concluded with our data processor, to the extent included therein.

### **7.1 Monitoring, checking, and inner audits**

(1) The responsible managers of each data processing department continuously monitor the compliance with the provisions of data protection regulations, especially this Policy and its related documents. Prior to the audit the Data Protection Officer, in legal cooperation with the Legal Director, shall provide the regional managers with the appropriate professional assistance and the priorities on which basis the audit will be carried out.

(2) The list of these responsible persons can be found in Appendix no. 26 of this Policy.

(3) Each data processing operation is checked as necessary, but at least once a year.

(4) The Data Protection Officer shall inform the chief executive director in writing about the observations and experience of the checking.

(5) Before preparing the information in writing, the Data Protection Officer shall consult the Legal Director and the head of each departments, and make a proposal to the chief executive director to take the necessary measures.

(6) The executive director shall be responsible for implementing the measures identified during the checking.



## 7.2 Adatvagyonleltár készítése

(1) Társaságunk adatvagyon leltárt készít. Az adatvagyon leltár tartalmazza a Társaságunk által kezelt összes adatkört, adatkörönként meghatározva – többek között –:

- a. az érintettek körét;
- b. az adatkezelés megnevezését és célját;
- c. a kezelt adatok körét (például név, születési időpont, lakcím, telefonszám, stb.);
- d. esetlegesen kezelt különleges adatok körét (például egészségügyi adatokat);
- e. az adatkezelés jogalapját (GDPR 6. cikk (1) bekezdés);
- f. az adatkezelés időtartamát;
- g. kik férhetnek hozzá a személyes adatokhoz a HCEMM Nonprofit Kft. szervezetén belül;
- h. kik számára kerülhet az adat továbbításra;
- i. alkalmaz-e a HCEMM Nonprofit Kft. adatfeldolgozót, ha igen, akkor pedig kit, milyen célra, milyen személyes adatokhoz férhet hozzá, mennyi ideig tárolhatja a személyes adatokat stb.

## 7.3 Adatvédelmi oktatás

(1) A HCEMM Nonprofit Kft. számára alapvető céltűzés, hogy a munkatársaink megismerjék és munkájuk, feladataik ellátása során helyesen és következetesen alkalmazzák az adatkezeléssel, valamint az adatvédelemmel kapcsolatos lényeges szabályokat, illetve a szabályzatainkban (így különösen a jelen Szabályzat, az IBSZ, valamint az Incidenskezelési Szabályzat) lefektetett eljárásrendet.

(2) Az adatvédelmi és adatbiztonsági ismeretekről a HCEMM Nonprofit Kft. a munkatársakat belépéskor, majd éves rendszerességgel oktatásban és továbbképzésben részesíti.

(3) A jelen Szabályzat és a kapcsolódó adatvédelmet érintő Szabályzatok hatálybalépése előtt is oktatásra kerül sor, amely oktató anyag elsajátítását az előadáson résztvevők aláírásukkal is igazolnak.

(4) Az évente, az Adatvédelmi Tisztviselő által tartandó megújító oktatások során az új folyamatok, szabályzatok bemutatásra kerülnek.

## **8. FEJEZET - AZ ADATTOVÁBBÍTÁSRA VONATKOZÓ SZABÁLYOK, ADATKEZELÉSI MŰVELETEK NYILVÁNTARTÁSA**

(1) A HCEMM Nonprofit Kft. által kezelt adatok akkor továbbíthatók, valamint a különböző adatkezelések akkor kapcsolhatók össze, ha az érintett ahhoz hozzájárult, vagy törvény azt megengedi, és ha az adatkezelés feltételei minden egyes személyes adatra nézve teljesülnek.

## 7.2 Data asset inventory

(1) Our Company prepares a data asset inventory. The data asset inventory includes all data sets processed by our Company, defined for each data set, such as – among other things –:

- a. the data subjects;
- b. the name and purpose of the data processing;
- c. the scope of the data processed (e.g. name, date of birth, address, phone number, etc.);
- d. the scope of specific data that may be processed (such as health data);
- e. the legal basis of the data processing (Section 1 of Article 6 of the GDPR);
- f. the duration of the data processing;
- g. those who can access personal data within the organisation of HCEMM Non-profit Kft;
- h. to whom the data may be transferred;
- i. whether the HCEMM Non-profit Kft. uses a data processor and, if so, who is it, for what purpose, what personal data it can access, for how long it can store personal data, etc.

## 7.3 Data protection training

The fundamental objective of HCEMM Non-profit Kft. is that, during their work, our Employees acquaint themselves with and are able to correctly and consistently apply the relevant rules related to data processing, data protection and our policies (especially this present Policy, the ISP, and the Incident Management Policy of HCEMM).

HCEMM Non-profit Kft. provides its employees with education and further training on data protection and data security upon entry and, subsequently, annually.

Training will also take place before this Policy and the related data protection regulations enter into force; the receipt of the training material will be confirmed by the signatures of the participants.

During the annual renewal trainings held by the Data Protection Officer, the new processes and regulations are presented.

## **ARTICLE 8 - RULES CONCERNING DATA TRANSFER, RECORDS OF DATA PROCESSING OPERATIONS**

(1) The data processed by HCEMM Non-profit Kft. may only be transferred and various data processing operations may only be combined if the data subject has consented to it or it is permitted by law, and if the conditions of data processing are met for each and every personal data.



(2) A 23. számú mellékletben felsorolt adatkezelési műveletek mellett, a HCEMM Nonprofit Kft. által végzett adattovábbítási műveletek kiemelendők:

- a. A személyes adatok továbbítása adatfeldolgozón kívüli, harmadik személyek számára;
- b. Az Európai Unión kívüli országba vagy nemzetközi szervezetek felé irányuló adattovábbítás.

(3) Az adatfeldolgozásra irányuló adatátadás nem minősül adattovábbításnak.

(4) Az EGT-államba irányuló adattovábbítást úgy kell tekinteni, mintha Magyarország területén belüli adattovábbításra kerülne sor.

#### 8.1 A személyes adatok továbbítása adatfeldolgozón kívüli, harmadik személyek számára

(1) Társaságunk minden adatkezelést végző munkavállalója, alkalmazottja a szerződött adatfeldolgozóktól eltérő személyektől érkező, adattovábbításra irányuló megkeresésről haladéktalanul tájékoztatja a szervezeti egysége felelős vezetőjét (26. számú mellékletben lévő listában szereplő személyeket). Az egység vezetője a rendelkezésre álló adatok alapján megvizsgálja az adattovábbítás feltételeinek fennállását, a kérés teljesíthetőségét, szükség esetén további tájékozódást végez a megkereső személyről, az adatok típusáról, jellegéről és egyéb lényeges tényezőkről.

(2) Az egység vezetője írásban vagy elektronikus úton tájékoztatja az Adatvédelmi Tisztviselőt. Az adatok továbbításának feltételeinek fennállását az Adatvédelmi Tisztviselő megvizsgálja, és ennek alapján 15 munkanapon belül javaslatot tesz az adattovábbítás végrehajthatóságáról.

#### 8.2 Az Európai Unión kívüli országba vagy nemzetközi szervezetek felé irányuló adattovábbítás

(1) A Társaságunk valamely alkalmazottja, által kezelt személyes adatokat az Európai Unión kívüli harmadik országba, vagy nemzetközi szervezetek számára abban esetben továbbíthat, ha:

- a. az Európai Unió Bizottsága határozatával megállapította, hogy a harmadik ország, a harmadik ország valamely területe; vagy egy vagy több meghatározott ágazata, vagy a szóban forgó nemzetközi szervezet megfelelő védelmi szintet biztosít. Az ilyen adattovábbításhoz nem szükséges külön engedély; vagy
- b. a harmadik országbeli, vagy nemzetközi szervezetnek minősülő adatkezelő vagy adatfeldolgozó a GDPR 46. cikkében foglalt megfelelő garanciákat nyújtott, és csak azzal a feltételel, hogy az érintettek számára érvényesíthető jogok és hatékony jogorvoslati lehetőségek állnak rendelkezésre. A garanciáktól függően szükséges, vagy elhagyható az illetékes felügyeleti hatóság engedélye.

(2) A fenti adatszolgáltatással kapcsolatos tényeket, körülményeket dokumentálni kell, melynek formalitását az Adatvédelmi Tisztviselővel együttműködve készítik el.

(2) In addition to the data processing operations listed in Appendix no. 23, data transfer operations performed by HCEMM Non-profit Kft. should be highlighted:

- a. Transfer of personal data to a third party other than the processor;
- b. Transfer of data to countries outside of the EU or to international organisations.

(3) Data transmission for the purpose of data processing is not considered as data transfer.

(4) Transfer of data to an EEA state shall be considered equivalent to transferring data within the territory of Hungary.

#### 8.1 Transfer of personal data to a third party other than the processor

(1) Every employee of our Company performing data processing shall immediately inform the head of their organisational unit (persons listed in Appendix no. 26) of any data transfer request coming from persons other than the contracted data processors. Based on the data available, the head of the unit examines the existence of the conditions for the data transfer, the feasibility of the request, and if necessary, provides additional information about the requesting person, the type and nature of the data and other relevant factors.

(2) The head of each department shall inform the Data Protection Officer in writing or electronically. The Data Protection Officer shall examine the existence of conditions for the transfer of data and, based on it, shall make a proposal within 15 working days regarding the feasibility of the data transfer.

#### 8.2 Transfer of data to countries outside of the EU or to international organisations

(1) An employee of our Company may transfer personal data to a third country outside of the EU or an international organisation only if:

a. the European Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation; or

b. a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards in accordance with Article 46 of the GDPR, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. Depending on the nature of the safeguards, authorisation by the competent supervisory authority should be obtained or omitted.

(2) The facts and circumstances related to the data provision above shall be documented and prepared in cooperation with the Data Protection Officer.





(3) Az Unió Bizottságának megfelelőségi határozata, illetve a GDPR 46. cikk szerinti megfelelő garanciák hiányában – beleértve a BRC-kötelező szervezeti szabályozást is –, a személyes adatok harmadik ország vagy nemzetközi szervezet részére történő továbbítására, vagy többszöri továbbítására csak az alábbi feltételek legalább egyikének teljesülése esetén kerülhet sor:

- a. az érintett kifejezetten hozzájárulását adta a tervezett továbbításhoz azt követően, hogy tájékoztatták az adattovábbításból eredő – a megfelelőségi határozat és a megfelelő garanciák hiányából fakadó – esetleges kockázatokról;
- b. az adattovábbítás az érintett és a Társaság közötti szerződés teljesítéséhez, vagy az érintett kérésére hozott, szerződést megelőző intézkedések végrehajtásához szükséges;
- c. az adattovábbítás a Társaság és valamely más természetes vagy jogi személy közötti, az érintett érdekét szolgáló szerződés megkötéséhez vagy teljesítéséhez szükséges;
- d. az adattovábbítás fontos közérdekből szükséges; (a jelen pontban foglalt közérdeket akkor kell figyelembe venni, ha azt az uniós jog vagy a Társaságra vonatkozó tagállami jog elismeri);
- e. az adattovábbítás jogi igények előterjesztése, érvényesítése és védelme miatt szükséges;
- f. az adattovábbítás az érintett vagy valamely más személy létfontosságú érdekeinek védelme miatt szükséges, és az érintett fizikailag vagy jogilag képtelen a hozzájárulás megadására;
- g. a továbbított adatok olyan nyilvántartásból származnak, amely az uniós vagy a tagállami jog értelmében a nyilvánosság tájékoztatását szolgálja, és amely vagy általában a nyilvánosság, vagy az ezzel kapcsolatos jogos érdekét igazoló bármely személy számára betekintés céljából hozzáférhető, de csak ha az uniós vagy tagállami jog által a betekintésre megállapított feltételek az adott különleges esetben teljesülnek. A jelen pont szerinti adattovábbítás nem érintheti a nyilvántartásban szereplő személyes adatok vagy személyes adatok kategóriáinak összességét. Ha a nyilvántartásba kizárolag olyan személyek tekinthetnek be, aiknek ehhez jogos érdeke fűződik, az adattovábbításra kizárolag e személyek kérelmére kerülhet sor, illetve abban az esetben, ha ők a címzettek.

(4) Ha az adattovábbítás nem alapulhat a megfelelőségi határozaton, vagy a GDPR-ban meghatározott garanciákon és a fentiekben említett egyedi helyzetekre vonatkozó eltérések egyike sem alkalmazandó, harmadik országok és nemzetközi szervezetek részére történő adattovábbítás csak akkor történhet, ha az adattovábbítás nem ismétlődő, csak korlátozott számú érintette vonatkozik, a Társaság olyan kényszerítő erejű jogos érdekében szükséges, amely érdekhez képest nem élveznek elsőbbséget az érintett érdekei, jogai és szabadságai, és a Társaság az adattovábbítás minden körülményét megvizsgálta, és e vizsgálat alapján megfelelő garanciákat nyújtott a személyes adatok védelme tekintetében. A Társaság a vizsgálatot és megfelelő garanciákat az adatkezelési tevékenységek nyilvántartásában dokumentálja.

(3) In the absence of an adequacy decision of the Commission, or of appropriate safeguards pursuant to Article 46 of the GDPR, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions:

- a. the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
- b. the transfer is necessary for the performance of a contract between the data subject and the Company or the implementation of pre-contractual measures taken at the data subject's request;
- c. the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the Company and another natural or legal person;
- d. the transfer is necessary for important reasons of public interest (the public interest referred to in this section shall be recognised in the EU law or in the law of the Member State to which the controller is subject);
- e. the transfer is necessary for the establishment, exercise or defence of legal claims;
- f. the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;
- g. the transfer is made from a register which according to EU or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case. A transfer pursuant to this section shall not involve the entirety of the personal data or entire categories of the personal data contained in the register. Where the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.

(4) Where a transfer could not be based on the adequacy decision or the safeguards defined in the GDPR, and none of the derogations for a specific situation referred to in the first subparagraph of this paragraph are applicable, a transfer to a third country or an international organisation may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the Company which are not overridden by the interests or rights and freedoms of the data subject, and the Company has assessed all the circumstances surrounding the data transfer and has, on the basis of that assessment, provided suitable safeguards with regard to the protection of personal data. The Company shall document the assessment as well as the suitable safeguards referred in the records of processing activities.



(5) A Társaságunknak tájékoztatnia kell a NAIH-ot az adattovábbításról.

(6) Megfelelőségi határozat hiányában az uniós jog vagy a tagállami jog fontos közérdekből kifejezetten korlátozhatja bizonyos kategóriákba tartozó személyes adatok valamely harmadik országba vagy nemzetközi szervezethez történő továbbítását.

### 8.3 Adattovábbítás szegmensei:

(1) A HCEMM Nonprofit Kft. egy H2020 program keretében megvalósuló kutatás-fejlesztést megvalósító projekt. A HCEMM Nonprofit Kft. koordinálása alatt működő konzorcium – a Szegedi Tudományegyetem, a Szegedi Biológiai Kutatóközpont, a Semmelweis Egyetem és az EMBL – célja egy olyan kiválósági központ létrehozása, amely kutatócsoportokat fogad be, előre rögzített időtartamra.

(2) Ismert, hogy a Társaság tevékenysége során szoros együttműködésben áll több EGT tagállamban honos gazdasági Társasággal, intézménynel. A konzorciumi szerződés, szindikációs szerződés, valamint a partner szervezetekkel és intézményekkel való együttműködési gyakorlatok, együttműködési megállapodás alapján, és a velük fennálló szerződések viszonyból kifolyólag kölcsönös adatközlésre és egyedi adatkezelési műveletekre kerül sor. Ez megalapozza más hazai, és külföldi illetőségű gazdasági Társaságok, szervezetek, intézmények részére történő rendszeres adatszolgáltatást.

### 8.4 Adatkezelési tevékenységek nyilvántartása és Adattovábbítási nyilvántartás

(1) HCEMM Nonprofit Kft. az elszámoltathatóság elvének megfelelően végzi az adatkezelési tevékenységek nyilvántartását annak érdekében, hogy az GDPR-nak való megfelelést igazolni tudja, ami az alábbi pontokat foglalja magába (23. számú melléklet):

- a. a Társaság neve és elérhetősége, valamint – ha van ilyen – a közös adatkezelőnek, a Társaság képviselőjének és az Adatvédelmi Tisztviselőnek a neve és elérhetősége;
- b. az adatkezelés céljai;
- c. az érintettek kategóriáinak, valamint a személyes adatok kategóriáinak ismertetése;
- d. olyan címzettek kategóriái, akikkel a személyes adatokat közlik vagy közölni fogják, ideértve a harmadik országbeli címzetteket vagy nemzetközi szervezeteket;
- e. adott esetben a személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információk, beleértve a harmadik ország vagy a nemzetközi szervezet azonosítását, valamint a GDPR 49. cikk (1) bekezdésének második albekezdés szerinti továbbítás esetében a megfelelő garanciák leírása;
- f. ahol lehetséges, a különböző adatkategóriák törlésére előírányzott határidők;
- g. ahol lehetséges, a GDPR 32. cikk (1) bekezdésében említett technikai és szervezési intézkedések általános leírását.

(2) HCEMM Nonprofit Kft. adattovábbítási nyilvántartást vezet annak érdekében, hogy az adattovábbítás jogosrólégtétel ellenőrizze, valamint, hogy az érintett tájékoztassa. Ez

(5) Our Company shall inform NAIH about the transfer of data.

(6) In the absence of an adequacy decision, EU or Member State law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of personal data to a third country or an international organisation.

### 8.3 Segments of data transfer:

(1) HCEMM Non-profit Kft. is a research and development project implemented within the framework of the H2020 programme. The consortium - the University of Szeged, the Biological Research Centre (Szeged), the Semmelweis University and the EMBL- coordinated by the HCEMM Non-profit Kft. and aims to create a centre of excellence that hosts research groups for a pre-set period of time.

(2) It is known that in the course of its activities the Company cooperates closely with companies and institutions resident in several EEA member states. Based on the consortium agreement, the syndicate agreement and the cooperation practices with the partner organisations and institutions, and due to the cooperation agreement and the contractual relationship with them, mutual communication and individual data processing operations will take place. This establishes the regular provision of data to other domestic and foreign resident companies, organisations and institutions.

### 8.4 Records of data processing activities and register of data transfer

(1) HCEMM Non-profit Kft. carries out the registration of data processing activities in accordance with the principle of accountability, in order to be able to verify compliance with the GDPR, which includes the following sections (Appendix no. 23):

- a. the name and contact details of the Company and, where applicable, the joint controller, the controller's representative and the Data Protection Officer;
- b. the purposes of the data processing;
- c. a description of the categories of data subjects and of the categories of personal data;
- d. the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;
- e. where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49 (1) of the GDPR, the documentation of suitable safeguards;
- f. where possible, the envisaged time limits for erasure of the different categories of data;
- g. where possible, a general description of the technical and organisational security measures referred to in Article 32(1) of the GDPR.

(2) HCEMM Non-profit Kft. maintains a record of data processing activities in order to verify the legality of the transfer and to inform the data subject. This includes the date of the transfer



tartalmazza az általa kezelt személyes adatok továbbításának időpontját, az adattovábbítás jogalapját és címzettjét, a továbbított személyes adatok körének meghatározását, valamint az adatkezelést előíró jogszabályban meghatározott egyéb adatokat.

(3) A HCEMM Nonprofit Kft. az adatkezelési tevékenységekről elsősorban az alábbi nyilvántartásokat vezeti:

- a. érintetti jogok érvényesítése iránti igények, kérelmek, valamint az arra a HCEMM Nonprofit Kft. által adott válaszok nyilvántartása;
- b. tájékoztatási kötelezettség megtagadási nyilvántartás;
- c. hatósági igények, kérelmek, megkeresések és az arra a HCEMM Nonprofit Kft. által adott válaszok nyilvántartása;
- d. adattovábbítási nyilvántartás;
- e. adatkezelés megszüntetése iránti kérelmek nyilvántartása;
- f. Munkavállalói tájékoztató a munkaviszonnyal kapcsolatos személyes adatok kezeléséről;
- g. Adatvédelmi incidens nyilvántartása;
- h. A HCEMM Nonprofit Kft.-hez álláspályázatot benyújtók személyes adatainak nyilvántartása.

## **9. FEJEZET - TÁRSASÁGUNK MUNKAVÁLLALÓIRA VONATKOZÓ ADATOK KEZELÉSE**

(1) A munkavállalóink adatainak kezelése kapcsán adatgazdának minősül a HCEMM Nonprofit Kft. vezetője, továbbá minden olyan szervezeti egység vezetője, aiknek az irányítása alatt álló szervezeti egységnél munkavállalói adatokat kezelnek.

### 9.1 A munkahelyi adatkezelés alapelvei

(1) HCEMM Nonprofit Kft. a munkavállalóktól kizárolag olyan adatokat kér be és olyanok tarthatók nyilván, illetve olyan munkaköri alkalmassági vizsgálatok végezhetők, amelyek az adott munkavállaló munkaviszonyának létesítéséhez, fenntartásához és megszüntetéséhez, valamint a szociális-jótéti juttatások biztosításához szükségesek és a munkavállaló személyhez fűződő jogait nem sértik.

### 9.2 A munkahelyi adatkezelés jogalapja, a munkavállalókkal kapcsolatos adatkezelés jogalapja

(1) Az érintett hozzájárulása, amennyiben az adatkezelés nem a munkaviszonnyal összefüggésben jött létre. A hozzájárulás megtagadása nem okozhat a munkavállalónak semmiféle hátrányt.

(2) Jogi kötelezettség.

of the personal data processed, the legal basis and the recipient of the transfer, the definition of the scope of the transferred personal data, as well as the other data specified in the legislation prescribing data processing.

(3) HCEMM Non-profit Kft. keeps mainly the following records on data processing activities:

- a. record of claims and requests of enforcement of rights of the data subjects, and the responses of HCEMM Non-profit Kft.;
- b. record of refusal of undertaking to provide information;
- c. record of official claims, requests and inquiries and the responses given by HCEMM Non-profit Kft.;
- d. record of transfer of data;
- e. record of requests for termination of data processing;
- f. Employee policy on the processing of personal data related to the employment relationship;
- g. record of personal data breach;
- h. record of personal data of people submitting job applications to HCEMM Non-profit Kft.

## **ARTICLE 9 - PROCESSING THE DATA OF OUR COMPANY'S EMPLOYEES**

(1) Regarding the data processing of our employees, the chief executive officer of HCEMM Non-profit Kft. and the heads of all organisational units under whose control employee data is processed, qualify as the data owner.

### 9.1 Principles of data processing at work

(1) HCEMM Non-profit Kft. shall request data from employees and keep records only of such data, and shall perform only such job competency tests, that are necessary for the establishment, maintenance and termination of the employment relationship of the employee, as well as for the provision of social welfare benefits, and that do not violate the employee's personal rights.

### 9.2 Legal basis of data processing at work, legal basis of employee related data processing

(1) Consent of the data subjects, if the data processing was not established in relation with the employment relationship. Refusal of consent shall not cause any disadvantage to the employee;

(2) Legal obligation.



(3) Társaságunk, mint munkáltató jogos érdeke, amely jogalap a munkavállalók hozzájárulásától függetlenül jogosítja teheti az adatkezelésünket akkor, ha a jogos érdekkünk arányosan korlátozza a munkavállalók személyes adatok védelméhez való jogát, magánszféráját.

(4) A HCEMM Nonprofit Kft. a jogalap meghatározásakor a jogos érdek, mint jogalap esetén figyelembe veszi a jogszabályok előírásait, illetve az érintettek érdekeit, valamint jogait és ezek alapján ötlépéses érdekmérlegelési tesztet végez.

(5) Az előzetes tájékoztatás követelményéből fakadóan követelmény, hogy

a. az érintett az előzetes és megfelelő tájékoztatás alapján képes legyen felismerni azt, hogy az adott adatkezelés milyen hatással van az információs önrendelkezési jogára és a magánszférájára;

b. az előzetes, megfelelő tájékoztatás kötelezettségének központi eleme a GDPR és az Info tv., amelyek felsorolják azokat az alapvető adatkezelési körülmenyeket, amelyekről az adatkezelőnek tájékoztatást kell nyújtania;

c. amennyiben a munkáltató technikai eszközzel kíván ellenőrzést végezni, úgy az nem lehet titkos, arról a munkavállalókat előzetesen tájékoztatni kell;

d. kiemelten fontos arról is tájékoztatást nyújtani, hogy Társaságunk szervezetrendszerén belül ki férhet hozzá a személyes adatokhoz. Azt a személyi kört, akik hozzáférhetnek a személyes adatokhoz, adatkezelési célonként külön-külön kell meghatározni. Társaságunk törekszik az adatkezelés szüksességgével-arányosságával kapcsolatos garanciák biztosítására, így az ellenőrzés során fokozatosan elvénék érvényesítésére, a munkavállaló jelenlétének lehetővé tételeire.

### 9.3 Előzetes tájékoztatási kötelezettség

(1) Társaságunk az adatkezelési folyamat megkezdése előtt közli a munkavállalóval azt, hogy az adatkezelés hozzájáruláson, jogos érdeken alapul vagy kötelező.

(2) Az adatkezelés megkezdése előtt egyértelműen és részletesen tájékoztatjuk az egyes munkavállalót 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.

(3) A tájékoztatás kiterjed az érintett adatkezeléssel kapcsolatos jogaira és jogorvoslati lehetőségeire is. Arról is tájékoztatjuk a munkavállalót, hogy Társaságunk szervezetrendszerén belül ki férhet hozzá a személyes adatokhoz. Azt a személyi kört, akik hozzáférhetnek a személyes adatokhoz, adatkezelési célonként külön-külön kell meghatározni.

(4) Társaságunk a személyiségi jog korlátozásának módjáról, feltételeiről és várható tartamáról előzetesen tájékoztatja a munkavállalót, valamint azoknak a technikai eszközöknek az alkalmazásáról is, amelyek a munkavállaló ellenőrzésére szolgálnak.

(3) The legitimate interest of our Company, which can make our data processing lawful regardless of the consent of the employees, if our legitimate interest proportionally restricts the right of privacy of the employees to the protection of personal data.

(4) When determining the legitimate interest as legal basis, HCEMM Non-profit Kft. takes the provisions of legal regulations and the interests and rights of the data subjects into account, and performs a five-step interest balancing test based on these.

(5) As a result of the prior information requirement, it is a requirement that:

a. based on prior and adequate information, the data subject shall be able to identify the effect of data processing on his or her right to information self-determination and privacy;

b. the key elements of the obligation of prior and adequate information are GDPR and the Info tv., which list those basic data processing conditions of which the controller shall provide information;

c. in case the employer wishes to carry out a check by technical means, it shall not be confidential, and the employees shall be informed in advance;

d. it is also of the utmost importance to provide information on who can access personal data within the organisational system of our Company. Those persons who may have access to personal data shall be defined separately for each data processing purpose. Our Company strives to provide safeguards related to the necessity and proportionality of data processing, thus to enforce gradualism during the checking and enable the presence of the employee.

### 9.3 Prior information obligation

(1) Before starting the process of data processing, our Company informs the employee if the data processing is based on consent, on legitimate interest or is mandatory.

(2) Before starting the process of data processing, we provide clear and detailed information to each employee about all the facts related to the processing of their data, in particular the purpose and legal basis of the data processing the person authorised for the processing and management of data, the duration of data processing and by whom the data will be viewed.

(3) The information shall also cover the data subject's rights and remedies. We also inform the employee about who can access the personal data within the organisational system of our Company. Those persons who may have access to personal data shall be defined separately for each data processing purpose.

(4) Our Company informs the employee in advance about the manner, conditions and expected duration of the restriction of the rights relating to personality, as well as about the application of the technical means used for checking the employee.



#### 9.4 Felvételre jelentkező munkavállalók személyes adatainak kezelése

(1) A felvételi eljárás során a jelentkezők kezelhető személyes adatai:

- a. név;
- b. születési idő és hely;
- c. anyja neve;
- d. lakcím;
- e. képesítési adatok;
- f. telefonszám és e-mail cím;
- g. a jelentkezőről készített munkáltatói feljegyzés (amennyiben készült ilyen).

(2) Társaságunk nem alkalmaz anonim álláshirdetéseket.

(3) Amennyiben a HCEMM Nonprofit Kft. megtekinti a jelentkezők közösségi oldalon közzétett profilját és az ott nyilvánosan elérhető adatait, akkor előzetes tájékoztatás keretében ismertetjük a jelentkezőkkel, hogy a felvételi eljárás folyamata kiterjed erre az információra is.

(4) A közösségi oldalakon közzétett, de csupán korlátozottan nyilvános adatokat Társaságunk nem ismeri meg, arra irányuló adatkeresést nem végez.

(5) Társaságunk kizárolag azokat az információkat ismerheti meg, amelyek lényegesen az álláspályázattal vagy munkakörrel kapcsolatban, és egyúttal vállaljuk, hogy a jelentkező profiloldalát nem mentjük le és azt nem tároljuk.

(6) A személyes adatok kezelésének célja a jelentkezések, pályázatok elbírálása, a kiválasztott leendő munkavállalóval szerződés kötése.

(7) Társaságunk nem vállal kötelezettséget a tekintetben, hogy minden jelentkezőt értesít arról, hogy nem őt választotta az adott állásra. Az adatkezelés jogalapja az érintett hozzájárulása, a személyes adataik címzettjei a Társaságunknál munkáltatói jog gyakorlására jogosult vezetők, illetve a munkaügyi feladatot ellátó munkavállalók.

#### 9.5 Feddhetetlen előélet igazolása

(1) Társaságunk a munkaviszony létesítése előtt, a felvételi eljárás során, illetőleg a munkaviszony fennállása alatt is felszólíthatja az érintettet a feddhetetlen előélet igazolására, amennyiben az erkölcsi alkalmasság igazolása valamely ágazati jogszabályban meghatározottak szerint az adott munkakör betöltéséhez elengedhetetlen. A hatósági erkölcsi bizonyítvány közikirat, melynek tartalmát Társaságunk köteles a kiállításától számított kilencven napig valósnak elfogadni. Társaságunk a munkavállalótól hatósági erkölcsi bizonyítvány helyett a bűnűgyi nyilvántartási rendszerben kezelt adataira vonatkozó tájékoztatást nem fogadhatja el, ilyen dokumentumból származó adatot nem kezelhet.

#### 9.4 Processing of personal data of candidates applying for employment

(1) Applicants' personal data to be processed during the recruitment procedure:

- a. name;
- b. date and place of birth;
- c. mother's name;
- d. home address;
- e. qualification data;
- f. telephone number and e-mail address;
- g. employer's record of the applicant (if any).

(2) Our Company does not use anonymous job advertisements.

(3) If HCEMM Non-profit Kft. views the profile of the applicants published on social media websites and the data publicly available there, we will inform the applicants in the framework of preliminary information that the process of the recruitment procedure also covers this information.

(4) Our Company does not get to know the data that is published on the social media with limited access, and does not search for such data.

(5) Our Company can only access information that is relevant to the job application or job position, and at the same time we undertake not to save or store the candidate's social media profile information.

(6) The purpose of processing personal data is to assess applications and tenders, and to enter into a contract with the selected prospective employee.

(7) Our Company has no obligation to notify all applicants that they have not been selected for the position. The legal basis of the data processing is the consent of the data subject. The recipients of the personal data are the managers authorised to exercise the employer's right at our Company, and the employees performing the labour task.

#### 9.5 Certification of being a person of integrity

(1) Before the establishment of the employment relationship, during the recruitment procedure, or during the existence of the employment relationship, our Company may require the data subject to certify his or her history of integrity, if proof of moral suitability is essential for filling the given position as defined in a sectoral law. Certificate of Good Conduct is a public document, the content of which our Company is obliged to accept as valid for ninety days from the date of its issuance. Our Company shall not accept information from the employee regarding his or her data processed in the criminal record system instead of an official Certificate of Good Conduct, nor shall it process data stemming from such a document.



## 9.6 Munkavállalók adatai

(1) Társaságunk az egyes munkavállalóira vonatkozó személyi nyilvántartásokban felsorolt adatokat kezelheti jogi kötelezettség teljesítése, illetve a munkáltatói jogos érdeke jogalap alapján, munkaviszony létesítése, teljesítése vagy megszűnése céljából.

(2) Társaságunk betegségre vonatkozó (különleges) adatokat csak a 2012. évi I. törvény a munka törvénykönyve szerinti meghatározott jog vagy kötelezettség teljesítése céljából kezelhet.

(3) A munkavállalóval az adatkezelés megkezdése előtt közölni kell, hogy az adatkezelés jogalapja a jogi kötelezettség teljesítése, illetve a munkáltató jogos érdeke.

(4) A munkáltató a munkaszerződés megkötésével egyidejűleg írásos tájékoztató átadásával tájékoztatja a munkavállalót a személyes adatainak kezeléséről és a személyhez fűződő jogairól.

(5) A munkavállalókkal kapcsolatban kezelt személyes adatak címzettjei a munkáltató vezetője, a munkáltatói jog gyakorlója, illetve a Társaságunk munkaügyi feladatokat ellátó munkavállalói és adatfeldolgozói.

(6) A Társaságunknál már egy korábbi adatbekérés miatt rendelkezésre álló személyes adatak többszöri, nem frissítés célú ismételt bekérése tilos. Kiemelendő, hogy az adatok ismételt megadásának megtagadása miatt munkavállalóinkat semmiféle hátrány nem érheti, erre Társaságunk kötelezettséget vállal.

(7) Társaságunk egyes munkavállalóinak adatait töröljük a személyi nyilvántartásból a munkaviszony megszűnését követő három év elteltével kivéve, ha a Társaságunk és a munkavállaló között ettől eltérő időtartalmú írásbeli megállapodás jön létre. De a törlési kötelezettség ezen opcionálisan megkötött írásbeli megállapodásban nem szereplő munkavállalói adatakre viszont kiterjed. Nem törölhetők a munkavállaló azon adatai a munkaviszony megszűnését követően sem, amelyek jogszabály alapján a továbbiakban is nyilvántarthatók vagy megőrzendők.

## 10. FEJEZET - AZ ADATKEZELÉS BIZTONSÁGA

(1) A HCEMM Nonprofit Kft. a kockázat mértékének megfelelő technikai és szervezési intézkedések alkalmazásával biztosítja az érintettek adatainak biztonságát, az adatak jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megszemmisítésével vagy károsodásával szembeni védelmet, ideértve a személyes adatak kezelésére használt informatikai rendszerek és eszközök bizalmasságának biztosítását, integritást, rendelkezésre állását és ellenálló képességét. Ennek érdekében a HCEMM Nonprofit Kft. többek között egy IBSZ szerkeszt a HCEMM Nonprofit Kft. IT menedzser vezetésével.

(2) Az IBSZ a Társaság engedélyezési és jogosultsággal kapcsolatos céljait támogatja a helyes, ellenőrzött és tudatos működés fenntartása érdekében. Az IBSZ célja egy egységes szabályozás kialakítása a Társaságon belül az engedélyezési és jogosultsági területeken, így csak az arra jogosult személyek rendelkezhetnek a Társaságnál a rendszerekhez és az információhoz hozzáféréssel. Az IBSZ megismerésével a vezetők és az alkalmazottak megismerik a feladatokat és a hozzá szükséges jogokat, elkerülhetők az ellentmondó vagy egymást kioltó jogosultságokkal rendelkező szerepkörök.

## 9.6 Data of employees

(1) Our Company may process the data listed in the personal records of each of its employees in order to fulfil the legal obligation or on the legal basis of the legitimate interest of the employer, for the purpose of establishing, fulfilling or terminating an employment relationship.

(2) Our Company may process (special) data on illness only for the purpose of fulfilling the right or obligation specified in the Act I of 2012 on the Labour Code.

(3) Before starting the data processing, the employee shall be informed that the legal basis of data processing is the fulfilment of the legal obligation or the legitimate interest of the employer.

(4) The employer informs the employee about the processing of their personal data and their moral rights by submitting a written notice at the same time as concluding the employment contract.

(5) The recipients of the personal data processed in connection with the employees are the head of the employer, the holder of the employer's right, and the employees and data processors of our Company performing labour tasks.

(6) It is prohibited at our Company to repeatedly request personal data that is already available due to a previous data request for non-update purposes. It should be emphasized that our employees cannot be disadvantaged in any way due to the refusal to provide the data repeatedly, our Company undertakes to not do so.

(7) The data of certain employees of our Company will be deleted from the personal register three years after the termination of the employment relationship, unless a written agreement of a different duration is concluded by and between our Company and the employee. However, the obligation to delete extends to employee data not covered by this optional written agreement. Even after the termination of the employment relationship, the employee's data that can still be registered or retained by law, shall not be deleted.

## ARTICLE 10 - SECURITY OF PROCESSING

(1) HCEMM Non-profit Kft. ensures the security of the data of the data subjects by applying appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including unauthorized or illegal processing of data, accidental loss of data, and the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services. To this end, HCEMM Non-profit Kft. maintains an ISP under the leadership of the IT Manager of HCEMM Non-profit Kft.

(2) ISP supports the Company's licensing and authorisation objectives in order to maintain proper, controlled and conscious operation. The purpose of the ISP is to establish a unified regulation within the Company in the areas of licensing and authorisation, so that only authorised persons can have access to the systems and information at the Company. By learning about ISP, managers and employees learn about the tasks and the rights required of them, and avoid roles with conflicting or mutually exclusive rights. It is important that all users shall be granted personal user rights, and that user rights shall be



Fontos, hogy valamennyi felhasználó személyre szóló felhasználói jogosultságot kell, hogy kapjon, továbbá a felhasználói jogosultságok kiadására, megváltoztatására, inaktiválására és törlésére is ezen IBSZ-ben részletezett eljárás szerint kell sor kerüljön.

(3) A HCEMM Nonprofit Kft. informatikai eszközöket, így különösen tűzfalakat, titkosítást, fizikai védelmi eszközöket használ rendszereiben, továbbá fizikai védelemmel látja el minden helyszíneket, ahol az adatok hozzáférhetők. A HCEMM Nonprofit Kft. az adatok biztonságát szolgáló intézkedések meghatározásakor és alkalmazásakor tekintetbe veszi a technika mindenkor fejlettségét. Több lehetséges adatkezelési megoldás közül azt választja (az aránytalan bekerülés esetét leszámítva), amely a személyes adatok magasabb szintű védelmét biztosítja.

## 10.1 Adatvédelmi incidens

(1) Az adatvédelmi incidens megfelelő és kellő idejű intézkedés hiányában fizikai, vagyoni vagy nem vagyoni károkat okozhat a természetes személyeknek, többek között a személyes adataik feletti rendelkezés elvesztését vagy a jogai korlátozását, a hátrányos megkülönböztetést, a személyazonosság-lopást vagy a személyazonossággal való visszaélést.

(2) A személyes adat jogellenes kezelése vagy feldolgozása esetén bejelentési kötelezettség keletkezik a Nemzeti Adatvédelmi és Információbiztonsági Hatóság, mint felügyelő hatóság felé. Az adatvédelmi incidenst a HCEMM Nonprofit Kft.-nek indokolatlan késedelem nélkül, legkésőbb 72 órán belül be kell jelentenie az illetékes felügyeleti hatóságnál (NAIH), kivéve, ha az elszámoltathatóság elvével összhangban bizonyítani lehet, hogy az adatvédelmi incidens valószínűleg nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Az érintett személyt késedelem nélkül tájékoztatni kell, ha az adatvédelmi incidenst valószínűsítetően magas kockázattal jár a természetes személy jogaira és szabadságára nézve, annak érdekében, hogy meg tudja tenni a szükséges óvintézkedéseket.

(3) A személyes adat jogellenes kezelése vagy feldolgozása esetén bejelentési kötelezettség keletkezik a Nemzeti Adatvédelmi és Információbiztonsági Hatóság, mint felügyelő hatóság felé. Az adatvédelmi incidenst a HCEMM Nonprofit Kft.-nek indokolatlan késedelem nélkül, legkésőbb 72 órán belül be kell jelentenie az illetékes felügyeleti hatóságnál (NAIH), kivéve, ha az elszámoltathatóság elvével összhangban bizonyítani lehet, hogy az adatvédelmi incidens valószínűleg nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Az érintett személyt késedelem nélkül tájékoztatni kell, ha az adatvédelmi incidenst valószínűsítetően magas kockázattal jár a természetes személy jogaira és szabadságára nézve, annak érdekében, hogy megtudja tenni a szükséges óvintézkedéseket.

(4) Lehetséges, hogy a HCEMM Nonprofit Kft. honlapján ([www.hcemm.eu](http://www.hcemm.eu)) valamilyen utalás, link található más szolgáltatók által fenntartott oldalakra (ideértve a bejelentkezési, megosztási lehetőségre mutató gombokat, logókat is), ahol az adatkezelő semmilyen befolyással nem bír a személyes adatok kezelésével kapcsolatos gyakorlatra. Az Adatkezelő felhívja az érintettek figyelmét, hogy ha ilyen linkekre kattintanak, más szolgáltatók oldalaira kerülhetnek át. Ilyen esetekben javasoljuk, hogy mindenfélekben olvassák el ezeknek az oldalaknak a használatára érvényes adatkezelési tájékoztatót. Jelen Szabályzat által folytatott adatkezelésre vonatkozik. Amennyiben bármilyen adatát az érintett külső

issued, changed, deactivated and deleted in accordance with the procedure detailed in this ISP.

(3) HCEMM Non-profit Kft. uses IT devices, such as firewalls, encryption, and physical protection devices in its systems, and also provides physical protection to all locations where the data is accessible. HCEMM Non-profit Kft. considers the current state of the development of technology when defining and applying data security measures. From several possible data processing solutions, we choose (except in the case of disproportionate access) that which provides a higher level of protection of personal data.

## 10.1 Personal data breach

(1) A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud.

(2) In case of unlawful management or processing of personal data, an obligation arises to notify the National Authority for Data Protection and Freedom of Information as a supervisory authority. HCEMM Non-profit Kft. shall report the personal data breach to the competent supervisory authority (NAIH), without undue delay and at the latest within 72 hours, unless it can be demonstrated, in accordance with the principle of accountability, that the personal data breach is not likely to pose a risk to the rights and freedoms of natural persons. The data subject shall be informed without delay if the personal data breach is likely to pose a high risk to the rights and freedoms of the natural person, in order to be able to take the necessary precautions.

(3) In connection with incident management, it should be emphasised that the processes concerning the handling of acts that violate data protection, the areas of responsibility and the necessary procedural order are recorded in the Incident Management Policy, which have been prepared by HCEMM Non-profit Kft. itself. Through incident management, HCEMM Non-profit Kft. aids the handling of events which violate data protection in connection with its operation in a unified system, preventing the development of acts violating data protection, detecting them in case of their occurrence, establishing liability and taking measures if necessary. The Incident Management Policy sets out the terminology, procedures and measures that ensure the prevention of the recurrence of events that violate data protection during the operation of the data controller, and the management of the detected events.

(4) It is possible that the website of HCEMM Non-profit Kft. ([www.hcemm.eu](http://www.hcemm.eu)) contains some reference to the pages maintained by other service providers (including buttons and logos pointing to the login and sharing option), where the data controller has no influence on the practice related to the processing of personal data. The data controller draws the attention of the data subjects to the fact that if they follow such links, they may be transferred to the pages of other service providers. In such cases, we recommend that you read the data processing policy of these sites. This Policy applies only to the data processing performed by the data controller. If the data subject modifies or deletes any of their data on an external



weboldalon módosítja, törli, az nem fogja érinteni az adatkezelő általi adatkezelést, az ilyen módosításokat a honlapon is el kell végeznie.

**11. FEJEZET - AZ ADATVÉDELMI TISZTVISELŐ  
KINEVEZÉSE ÉS ANNAK FELADATAI –  
A HCEMM NONPROFIT KFT. ADATVÉDELMI RENDSZERE,  
AZ ADATVÉDELMI TISZTVISELŐ JOGÁLLÁSA**

(1) Az ügyvezető a Társaságunk szervezetének sajátosságainak figyelembevételével meghatározza az adatvédelem feltételrendszerét, az adatvédelemre, valamint az azzal összefüggő tevékenységre vonatkozó feladat- és hatásköröket.

(2) Társaságunk valamennyi munkatársa (munkavállaló és megbízásos jogviszonyban tevékenykedő személyek egyaránt) munkájuk és feladataik ellátása során gondoskodnak arról, hogy jogosulatlan személyek ne tekinthessék be személyes adatokba, továbbá arról, hogy a személyes adat tárolása, elhelyezése úgy kerüljön kialakításra, hogy az jogosulatlan személy részére ne legyen hozzáférhető, megismerhető, megváltoztatható, megsemmisíthető.

(3) Társaságunk adatvédelmi rendszerének felügyeletét az ügyvezető látja el, az általa megbízott Adatvédelmi Tisztviselő útján.

(4) Az Adatvédelmi Tisztviselőt szakmai rátermettség és különösen az adatvédelmi jog és gyakorlat szakértői szintű ismerete, valamint az adatkezelés ellátására való alkalmasság alapján jelöli ki és bízza meg a HCEMM Nonprofit Kft.

(5) Társaságunk az Adatvédelmi Tisztviselő nevét és elérhetőségét jelen Szabályzatban, valamint honlapján elérhetővé teszi, és az illetékes felügyeleti hatóság (NAIH) részére bejelenti.

(6) A HCEMM Nonprofit Kft. biztosítja, hogy az Adatvédelmi Tisztviselő a személyes adatok védelmével kapcsolatos összes ügybe megfelelő módon és időben bekapcsolódjon. Biztosítani kell, hogy az Adatvédelmi Tisztviselő szakértői szintű ismereteinek fenntartásához szükséges források rendelkezésre álljanak.

(7) Az Adatvédelmi Tisztviselő a feladatai ellátásával kapcsolatban utasításokat senkitől nem fogadhat el. Társaságunk, az Adatvédelmi Tisztviselőt feladatai ellátásával összefüggésben nem bocsáthatja el és szankcióval sem sújthatja. Az Adatvédelmi Tisztviselő közvetlenül a ügyvezető felé tartozik felelősséggel.

(8) Az érintettek és adatalanyok a személyes adataik kezeléséhez és jogaiak gyakorlásához kapcsolódó valamennyi kérdésben az Adatvédelmi Tisztviselőhöz közvetlenül is fordulhatnak.

(9) Az Adatvédelmi Tisztviselőt feladatai teljesítésével kapcsolatban titoktartási kötelezettség terheli.

(10) Az Adatvédelmi Tisztviselő tájékoztatási és tanácsadási funkciót lát el Társaságunk teljes szervezete részére.

(11) Az Adatvédelmi Tisztviselő ellenőrzési feladataival elősegíti az adatvédelmi előírások (GDPR + Info tv., Társaság belső szabályzatai) érvényesülését.

website, it will not affect the data processing of the data controller, the data subject shall also make the modifications on the website.

**ARTICLE 11 - DESIGNATION AND TASKS OF THE DATA PROTECTION OFFICER – DATA PROTECTION SYSTEM OF HCEMM NONPROFIT KFT., POSITION OF THE DATA PROTECTION OFFICER**

(1) The chief executive officer determines the conditions of data protection, the tasks and powers related to data protection and the related activities, taking the specifics of the organisation of our Company into account.

(2) In the course of their work and duties, all employees of our Company (both employees and persons acting in a contractual relationship) ensure that unauthorized persons cannot access personal data, and that the storage and placement of personal data is designed in such a way that it is not accessible, cognisable, changeable or destructible to unauthorised persons.

(3) The data protection system of our Company is supervised by the chief executive officer, through the Data Protection Officer appointed by them.

(4) The Data Protection Officer is designated and entrusted by HCEMM Non-profit Kft. on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks related to data protection.

(5) Our Company publishes the contact details of the Data Protection Officer and communicates them to the competent supervisory authority (NAIH).

(6) HCEMM Non-profit Kft. shall ensure that the Data Protection Officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data. Resources necessary to carry out the tasks and access personal data and processing operations, and to maintain their expert knowledge, shall be provided.

(7) The Data Protection Officer shall not receive any instructions regarding the exercise of their tasks. The Data Protection Officer shall not be dismissed or penalised by our Company for performing their tasks. The Data Protection Officer shall directly report to the chief executive officer.

(8) Data subjects may contact the Data Protection Officer with regard to all issues related to the processing of their personal data and to the exercise of their rights under this Regulation.

(9) The Data Protection Officer shall be bound by confidentiality concerning the performance of their tasks.

(10) The Data Protection Officer performs informational and advisory tasks for the entire organisation of our Company.

(11) The Data Protection Officer facilitates the enforcement of data protection regulations (GDPR + Info tv., and the Company's internal regulations) with their control tasks.



(12) Az Adatvédelmi Tisztviselő hatásvizsgálattal kapcsolatos feladatai miatt Társaságunk köteles kikérni a tanácsát, továbbá az Adatvédelmi Tisztviselő nyomon követi a hatásvizsgálat lefolytatását is.

(13) Az Adatvédelmi Tisztviselőnek közvetítő és koordinációs szerepe van Társaságunk és annak adatfeldolgozói között, a felügyeleti hatóság (NAIH) és az érintettek között, de együttműködik a felügyeleti hatóságokkal is.

(14) Társaságunk az Adatvédelmi Tisztviselőt olyan egyéb feladatokkal is megbízza, mint például az adatalanyok részére nyújtott tanácsadás, érintetti panasz kivizsgálása, közreműködés a Társaságunk belső szabályzatainak elkészítésében, nyilvántartások vezetésének kontrollálásában.

(15) Az Adatvédelmi Tisztviselő ellátja Társaságunk hatályos Incidenskezelési Szabályzatában rögzített incidenskezelési feladatok koordinálását is.

(16) Az Adatvédelmi Tisztviselő tevékenységére a szelektív megközelítés elve irányadó, rangsorolja a tevékenységeit, és a magasabb kockázatot jelentő ügyekre fókusztálhat.

## **12. FEJEZET - ONLINE MEGJELENÉS, ÉS A COOKIE (SÜTI) KEZELÉS**

**(1) Internetes megjelenés:** A HCEMM Nonprofit Kft. az internetes honlapján közzéteszi az általános adatkezelési tájékoztatóját, melynek célja, hogy még az adatkezelés megkezdése előtt, illetve annak időtartama alatt az érintett megfelelő módon, egyértelműen és részletesen tájékozódhasson az adatainak kezelésével kapcsolatos minden tényről, így különösen:

- a. az adatai kezelésének céljáról és jogalapjáról;
- b. az adatkezelésre és adatfeldolgozásra jogosult személyek köréről;
- c. az adatkezelés időtartamáról;
- d. az adatok megismerésére jogosult személyek köréről;
- e. az érintett adatkezeléssel kapcsolatos jogaira és jogorvoslati lehetőségeire; valamint
- f. a vonatkozó főbb jogszabályi helyekről.

**(2) Intranet:** A Társaságunk jelenleg még nem üzemeltet intranetet, ennek informatikai lefejlesztése a jelen Útmutató kiadásának időpontjában még folyamatban van.

**(3) Cookie-kezelés:** Tekintettel Társaságunk nemzetközi tevékenységére és jellegére, továbbá arra, hogy a weboldalunk kizártlag angol nyelven olvasható, a weboldalon található tartalmak mellett a Süti/Cookie kezelési szabályzatunkat (Cookies and privacy policy) is kizártlag angol nyelven ismerheti meg.

(12) Due to the duties of the Data Protection Officer related to data protection impact assessment, our Company is obliged to seek their advice. Moreover, the Data Protection Officer shall also monitor the performance of the data protection impact assessment.

(13) The Data Protection Officer has a mediating and coordinating role between our Company and its data processors, the supervisory authority (NAIH) and the data subjects, but also cooperates with the supervisory authorities.

(14) Our Company also entrusts the Data Protection Officer with other tasks, such as advising data subjects, investigating complaints from data subjects, contributing to the preparation of our Company's internal regulations, and controlling the keeping of records.

(15) The Data Protection Officer also coordinates the incident management tasks set out in our Company's applicable Incident Management Policy.

(16) The activities of the Data Protection Officer are governed by this Policy, by the principle of a selective approach, they shall prioritise their activities and focus on higher risk cases.

## **ARTICLE 12 - ONLINE PRESENCE, USAGE OF COOKIES**

**(1) Internet:** HCEMM Non-profit Kft. publishes its general data processing policy on its website, the purpose of which is to enable the data subject to be informed in an adequate, clear and detailed manner of all facts relating to the processing of their data, before and during the processing, in particular:

- a. the purpose and legal basis of the processing of their data;
- b. the persons entitled to data management and data processing;
- c. the duration of the data processing;
- d. the persons entitled to access the data;
- e. the data subject's rights and remedies in regard to data processing; and
- f. the main places where the relevant laws and regulations can be found.

**(2) Intranet:** Our Company does not currently operate an intranet, the IT development of an intranet is still in progress at the time of issuing this Policy.

**(3) Cookie management:** Due to the international activities and nature of our Company, as well as the fact that our website can only be read in English, in addition to the content on the website you can only read our Cookies and privacy policy in English.



## 13. FEJEZET - ÉRINTETTI JOGGYAKORLÁS RENDJE, AZAZ AZ ÉRINTETT SZEMÉLY KÉRELMEK KEZELÉSE

(1) Az érintett bármikor felvilágosítást kérhet a jelen Szabályzatban rögzített jogaival, illetve az érintettré vonatkozó adatkezeléssel kapcsolatban a Társaságunk központi elérhetőségeihez, vagy az Adatvédelmi Tisztviselőkhöz intézett kérelemmel.

(2) Önt, mint érintettet az általános adatvédelmi rendelet (GDPR) rendelkezéseivel összhangban a következő jogok illetik meg:

(3) Az alábbiakban szeretnénk további felvilágosítást nyújtani Társaságunk adatkezelésével kapcsolatos jogairól. Amennyiben ezen jogok valamelyikét igénybe szeretné venni, vegye fel velünk a kapcsolatot email-ben ([gdpr@hcemm.eu](mailto:gdpr@hcemm.eu)), vagy postai formában (HCEMM Nonprofit Kft., levelezési cím: 6723 Szeged, Római körút 21.).

A Társaságunkhoz adatvédelmi tárgyú kérdéssel fordulása esetén a védelme érdekében fenntartjuk magunknak a jogot, hogy egy folyamatban lévő megkeresés során további információkat szerezzen be a beazonosítás igazolásához.

(4) Társaságunk a kérelmező azonosítása érdekében ügynevezett „Kérelmi űrlap” kitöltését kérheti, melyre – a kézbesítéstől számított - 15 napos határidőt ad. Ez esetben az ügyintézési határidő meghosszabbodik a Kérelmi űrlap visszaküldésére nyitva álló határidővel. Amennyiben a Kérelmi űrlapot az érintett nem küldi vissza, és az érintett ezért nem azonosítható, és nem állapítható meg teljes bizonyossággal, hogy az érintett a saját magára, vagy meghatalmazójára vonatkozó adatkezeléssel kapcsolatos információt kér, a kérelmet el kell utasítani, az elutasítás indokát a kérelmezővel köznöi. Amennyiben tehát mégsem tudjuk Önt beazonosítani, visszautasítjuk az adatvédelmi megkeresés feldolgozását.

### 13.1 TÁJÉKOZTATÁSHOZ VALÓ JOG

(1) Kérelmére a Társaságunk, mint adatkezelő tájékoztatást ad az általunk kezelt, illetőleg az általunk megbízott adatfeldolgozó által feldolgozott adatokról, azok forrásáról, az adatkezelés céljáról, jogalapjáról, időtartamáról, az adatfeldolgozó nevéről, címéről és az adatkezeléssel összefüggő tevékenységről, az adatvédelmi incidens körülményeiről, hatásairól és az elhárítására megtett intézkedésekről, továbbá adattovábbítás esetén annak jogalapjáról és címzettjéről.

(2) Társaságunk ezt a tájékoztatást a megkeresés benyújtásától számított legrövidebb idő alatt, legfeljebb azonban 30 napon belül, közérthető formában adjá meg. Amennyiben a tájékoztatást kérő érintett az adott évben azonos adatkörre vonatkozó tájékoztatási kérelmet, megkeresést Társaságunkhoz még nem nyújtott be, akkor a tájékoztatás megadása ingyenes. Egyéb esetekben Társaságunk költségtérítést állapít meg.

(3) Amennyiben az általunk végzett adatkezeléssel kapcsolatban bármilyen kérdése merülne fel, a [gdpr@hcemm.eu](mailto:gdpr@hcemm.eu) címen tájékoztatást kérhet tőlünk.

## ARTICLE 13 - EXERCISE OF RIGHTS OF THE DATA SUBJECT, I.E. HANDLING THE REQUEST OF A DATA SUBJECT

(1) The data subject may - at any time - request information regarding their rights as set out in this Policy, or the data processing concerning the data subject, by requesting it via the central contact details of our Company or our Data Protection Officer.

(2) You have the following rights as a data subject in accordance with the provisions of the General Data Protection Regulation (GDPR):

(3) Below we would like to provide you further information about our Company's data processing rights. If you wish to exercise any of these rights, please contact us by email ([gdpr@hcemm.eu](mailto:gdpr@hcemm.eu)) or by post (HCEMM Non-profit Kft., mailing address: 6723 Szeged, Római körút 21.).

(4) If you wish to contact our Company regarding a data protection matter, for the protection of our Company we reserve the right to obtain additional information to verify your identification during an ongoing request. In order to identify the applicant, our Company may request the completion of a so-called "Application Form", for which we give a deadline of 15 days from the date of delivery. In this case, the administrative deadline will be extended by the deadline of returning of the Application Form. If the Application Form is not returned by the data subject and therefore the data subject cannot be identified and it cannot be established with absolute certainty that the data subject requests information concerning themselves or their proxy, the request shall be rejected, the reasons for the rejection shall be communicated to the applicant. Therefore, if we are unable to identify you, we will refuse to process your privacy request.

### 13.1 RIGHT TO INFORMATION

(1) Upon your request our Company, as a data controller, provides information on the data processed by us or processed by the data processor, about the source, purpose, legal basis and duration of the data processed, about the name and address of the data processor and their activities related to data processing, about the circumstances, effects and measures taken to remedy a personal data breach and, in the event of a transfer, its legal basis and the addressee.

(2) Our Company will provide this information in a comprehensible form as soon as possible after the submission of the request, but within a maximum of 30 days. If the person requesting the information has not yet submitted an information request or request to our Company regarding the same data set in the given year, the provision of the information is free of charge. In other cases, our Company will charge a fee.

(3) If you have any questions about our data processing, please contact us at [gdpr@hcemm.eu](mailto:gdpr@hcemm.eu).



## 13.2 HOZZÁFÉRÉSHEZ VALÓ JOG

(1) Ön, mint érintett jogosult arra, hogy Társaságunktól visszajelést kapjon arra vonatkozóan, hogy személyes adatai kezelése folyamatban vannak-e és ha ilyen adatkezelés folyamatban van, jogosult arra, hogy a személyes adatokhoz hozzáférést kapjon.

## 13.3 HELYESBÍTÉSHEZ VALÓ JOG

(1) Társaságunk, mint adatkezelő a pontatlan, vagy a valóságnak nem megfelelő személyes adatát helyesbíti, ha a valóságnak megfelelő személyes adat a rendelkezésünkre áll.

(2) Megfelelő beazonosítást követően kérheti tőlünk a megadott elérhetőségeken keresztül, hogy valamely adatát módosítsuk. Erről a kérelméről haladéktalanul, de legfeljebb 30 napon belül intézkedünk, az Ön által megadott e-mail elérhetőségre tájékoztatást küldünk.

## 13.4 TÖRLÉSHEZ VALÓ JOG

(1) Érintettként jogosult arra, hogy Társaságunktól, mint adatkezelőtől kérje az Önre vonatkozó személyes adatok törlését, feltéve ha:

- a. a személyes adatokra már nincs szükség abból a célból, amelyből azokat gyűjtöttük vagy más módon kezeltük;
- b. visszavonja az adatkezelés alapját képező hozzájárulását, és az adatkezelésnek nincs más jogalapja;
- c. érintettként Ön tiltakozik az adatkezelés ellen, és nincs elsőbbséget élvező jogoszerű ok az adatkezelésre;
- d. amennyiben a személyes adatait Társaságunk jogellenesen kezelné;
- e. a személyes adatait a Társaságunkra, mint Adatkezelőre alkalmazandó uniós vagy tagállami jogban előírt jogi kötelezettség teljesítéséhez törölni kell;
- f. a személyes adatok gyűjtésére információs társadalommal összefüggő szolgáltatások kínálásával kapcsolatosan került sor (GDPR 8 cikk 1. bekezdés).

(2) A fentiekben leírtak esetén, a jelen Szabályzatban megadott elérhetőségeken keresztül kérheti tőlünk adatainak a törlését. Amennyiben a törlésnek jogi akadálya nem merül fel, akkor ezt haladéktalanul, de legfeljebb 30 napon belül megte tesszük.

(3) Előbbieken túl Társaságunk köteles törölni a személyes adatait:

- a. amennyiben azok kezelése jogellenes;
- b. hiányos vagy téves- és ez az állapot jogoszerűen nem orvosolható -, feltéve, hogy a törlést törvény nem zárja ki;
- c. amennyiben az adatkezelés célja megszűnt vagy az adatok tárolásának törvényben meghatározott határideje lejárt;
- d. azt a bíróság vagy a Hatóság elrendelte.

## 13.2 RIGHT OF ACCESS

(1) As a data subject, you have the right to receive feedback from our Company as to whether your personal data is being processed. If such data is being processed, you are entitled to have access to your personal data.

## 13.3 RIGHT OF RECTIFICATION

(1) Our Company, as a data controller, will correct your inaccurate or untrue personal data if we have your accurate personal data.

(2) After proper identification, you can ask us to change any of your details via the contact details provided. We will take action on your request without delay, but within a maximum of 30 days, and we will send you information by e-mail.

## 13.4 RIGHT TO ERASURE

(1) The data subjects shall have the right to request from our Company the erasure of their personal data:

- a. if the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- b. you withdraw consent on which the processing is based, and where there is no other legal ground for the processing;
- c. you as the data subject object to the processing and there are no overriding legitimate grounds for the processing;
- d. your personal data have been unlawfully processed by our Company;
- e. your personal data have to be erased for compliance with a legal obligation in EU or Member State law to which our Company is subject;
- f. the personal data have been collected in relation to the offer of information society services referred to in Article 8 (1) of the GDPR.

(2) In cases defined above, you shall request the erasure of your data via the contact details provided in this Policy. If there is no legal impediment to erasure we will endeavour do so immediately, but within a maximum of 30 days.

(3) In addition to the aforementioned our Company shall erase your personal data if:

- a. the processing is unlawful;
- b. the data is incomplete or incorrect - and this condition cannot be legally remedied - provided that the erasure is not precluded by law;
- c. the purpose of data processing has ceased or the term of storage of data specified by law has expired;
- d. it has been ordered by a court or the Authority.



**(4) Az adatok törlése nem kezdeményezhető:**

- a. a véleménynyilvánítás szabadságához és a tájékozódáshoz való jog gyakorlása céljából;
- b. a személyes adatok kezelését előíró, az adatkezelőre alkalmazandó uniós vagy tagállami jog szerinti kötelezettség teljesítése, illetve közérdekből vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlása keretében végzett feladat végrehajtása céljából;
- c. népegészségügy területét érintő közérdek alapján;
- d. közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból, amennyiben a törléshez jog valószínűsítetően lehetetlenne tenné vagy komolyan veszélyeztetné ezt az adatkezelést; vagy
- e. jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez.

### 13.5 ADATKEZELÉS KORLÁTOZÁSHOZ VALÓ JOG

**(1)** Mint érintett jogosult arra, hogy kérésére a Társaságunk, mint adatkezelő korlátozza az adatkezelést, ha az alábbiak valamelyike teljesül:

- a. vitatja a személyes adatok pontosságát;
- b. az adatkezelés jogellenes, és Ön ellenzi az adatok törlését, és ehelyett kéri azok felhasználásának korlátozását;
- c. már nincs szükségünk a személyes adatokra adatkezelés céljából, de Ön, mint érintett igényli azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez; vagy
- d. tiltakozott az adatkezelés ellen; ez esetben a korlátozás arra az időtartamra vonatkozik, amíg megállapításra nem kerül, hogy a Mi, mint adatkezelő jogos indokaink elsőbbséget élveznek-e a Ön jogos indokaival szemben.

**(2)** Ha az adatkezelés az előzőek szerinti -a.)-d.) pontok bármelyike- korlátozás alá esik, az ilyen személyes adatokat a tárolás kivételével csak az Ön hozzájárulásával, vagy jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez, vagy más természetes vagy jogi személy jogainak védelme érdekében, vagy az Unió, illetve valamely tagállam fontos közérdekből lehet kezelní.

### 13.6 ADATHORDOZHATÓSÁGHOZ VALÓ JOG

**(1)** Ön, mint érintett jogosult arra, hogy az Önre vonatkozó, rendelkezésünkre bocsátott, automatizált módon kezelt személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja, továbbá jogosult arra, hogy ezeket az adatokat egy másik adatkezelőnek továbbítsa anélkül, hogy ezt akadályoznánk, amennyiben az adatkezelés a GDPR 6. cikk (1) bekezdésének a) pontja vagy a 9. cikk (2) bekezdésének a) pontja szerinti hozzájáruláson, vagy a 6. cikk (1) bekezdésének b) pontja szerinti szerződésen alapul.

**(4) Erasure of data cannot be initiated:**

- a. for exercising the right of freedom of expression and information;
- b. for compliance with a legal obligation which requires processing by EU or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of an official authority vested in the controller;
- c. for reasons of public interest in the area of public health;
- d. for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, in so far as the right to erase is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
- e. for the establishment, exercise or defence of legal claims.

### 13.5 RIGHT TO RESTRICTION OF PROCESSING

**(1)** The data subject shall have the right to obtain from our Company restriction of processing where one of the following applies:

- a. the accuracy of the personal data is contested by you as data subject;
- b. the processing is unlawful and you oppose the erasure of the personal data and request the restriction of their use instead;
- c. we no longer need the personal data for the purposes of the processing, but they are required by you as the data subject for the establishment, exercise or defence of legal claims;
- d. you objected to processing; pursuant to Article 21 (1) pending the verification of whether the legitimate grounds of our Company override those of the data subject.

**(2)** Where processing has been restricted under a)-d), such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the EU or of a Member State.

### 13.6 RIGHT TO DATA PORTABILITY

**(1)** You, as the data subject, shall have the right to receive the personal data concerning you, which you have provided to us, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where: the processing is based on consent pursuant to point (a) of Article 6 (1) of the GDPR or point (a) of Article 9 (2) of the GDPR or on a contract pursuant to point (b) of Article 6(1) of the GDPR.



(2) Az adatok hordozhatóságához való jog gyakorlása során jogosult arra, hogy – ha ez technikailag megvalósítható – kérje a személyes adatok adatkezelők közötti közvetlen továbbítását.

### 13.7 TILTAKOZÁSHOZ VALÓ JOG

(1) Ön, mint érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból bármikor tiltakozzon a személyes adatainak az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges kezelése ellen. Ezenben Társaságunk, mint adatkezelő a személyes adatokat nem kezelheti tovább, kivéve, ha bizonyítjuk, hogy az adatkezelést olyan kényszerítő erekjű jogos okok indokolják, amelyek elsőbbséget élveznek az Ön, mint érintett érdekeivel, jogaival és szabadságával szemben, vagy amelyek jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez kapcsolódnak.

(2) A GDPR szabályozza továbbá azt az esetet is, amikor a személyes adatok kezelése közvetlen üzletszerzés érdekében történik, ekkor Ön, mint érintett jogosult arra, hogy bármikor tiltakozzon az Önre vonatkozó személyes adatok e célból történő kezelése ellen, ideértve a profilalkotást is, amennyiben az a közvetlen üzletszerzéshez kapcsolódik.

### 13.8 JOGORVOLSATI LEHETŐSÉG

(1) A HCEMM Nonprofit Kft. valamennyi alkalmazottja és közvetlen szerződéses partnere különös figyelmet fordít a Társaságunkkal kapcsolatba kerülők személyes adatinak megfelelően magas szintű védelmére és biztonságára. Az adatbiztonság keretében törekünk arra, hogy hatékonyan megvédjük a magánszférat, ezért olyan eljárásokat és intézkedéseket vezettünk és vezetünk be a jövőben is, amelyek biztosítják a személyes adatainak sérthetetlenségét és megelőzhető a személyes adataihoz történő jogosulatlan hozzáférés.

**(2) Kérjük, hogy az észlelt jogellenes adatkezelés esetén értesítse Társaságunkat, így lehetőségünk nyílik arra, hogy haladéktalanul érdemi segítséget nyújthassunk az adott helyzetre és rövid időn belül helyreálljon a jogoszerű állapot. Az érintettek érdekében minden megteszünk, hogy a tapasztalt probléma a leggyorsabban és a legkisebb kellemetlenséggel megoldódjon.**

(3) Adott tehát a Társaságunkhoz és adatvédelmi tisztviselőkhöz fordulás joga, azaz bármilyen, adatkezeléssel kapcsolatos kérdéssel, észrevételellet kereshet minket az alábbi postacímén, e-mail címen és telefonszámon egyaránt.

(4) Adatvédelmi tisztviselőnk neve, elérhetősége, dr. Kianek Zoltán Róbert adatvédelmi szakjogász, e-mail: [adatbiztonsag@protonmail.com](mailto:adatbiztonsag@protonmail.com)

(5) Amennyiben az Ön megítélése alapján a jogoszerű állapot mégsem állítható helyre (Társaságunk erőfeszítése ellenére sem), ez esetben adott a lehetőség panasz benyújtására az illetékes felügyeleti hatósághoz, az alábbi elérhetőségeken:

(2) In exercising your right to data portability you shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

### 13.7 RIGHT TO OBJECT

(1) You, as the data subject, shall have the right to object, on grounds relating to your particular situation, at any time to processing of personal data concerning you. In this case our Company, as controller, shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

(2) GDPR also regulates that if personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.

### 13.8 LEGAL REMEDIES

(1) All employees and direct contractual partners of the HCEMM Non-profit Kft. pay extra attention to the high level of protection and security of the personal data of those who come into contact with our Company. As part of data security, we strive to effectively protect your privacy, and we have put in place, and will continue to put in place, procedures and measures that ensure the integrity of your personal information and prevent unauthorised access to your personal information.

**(2) Please notify our Company in the event of any detected unlawful data processing, so that we have the opportunity to provide substantive assistance to the situation immediately and to restore the lawful status within a short period of time. In the interest of the data subjects, we will do our best to solve the problem experienced as quickly as possible and with the least inconvenience.**

(3) Therefore, you have the right to contact our Company and our Data Protection Officer; you can contact us with any questions or comments related to data processing at our postal address, e-mail address and telephone number below.

(4) Name and contact details of our Data Protection Officer, dr. Kianek Zoltán Róbert - data protection lawyer, e-mail: [adatbiztonsag@protonmail.com](mailto:adatbiztonsag@protonmail.com)

(5) If, in your opinion, the legal status cannot be restored (despite the efforts of our Company), you have the opportunity to submit a complaint to the competent supervisory authority, via the following contact details:



**Nemzeti Adatvédelmi és Információszabadság Hatóság  
(NAIH)**

Postacím: 1530 Budapest, Pf.: 5.  
Cím: 1125 Budapest Szilágyi Erzsébet fasor 22/C.  
Telefon: 06-1/391-1400  
Fax: 36-1/391-1410  
E-mail cím: ugyfelszolgatal@naih.hu  
Weboldal: <http://naih.hu>

(6) Mint érintett, a jogai megsértése esetén Ön Társaságunk ellen bírósághoz is fordulhat, mely esetben a bíróság az adott ügyben soron kívül jár el.

**(7) TÁJÉKOZTATJUK, HOGY AZ ADATAINAK KEZELÉSÉT  
AZ ALÁBBI JOGSZABÁLYOK SZERINT KEZELJÜK, VAGY  
KEZELHETJÜK:**

- a. Magyarország Alaptörvénye, vonatkozó rendelkezések;
- b. AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet, azaz a GDPR);
- c. az információs önrögzítési jogról és az információszabadságról szóló 2011. évi CXII. törvény (Info tv.);
- d. A gazdasági reklámtevékenység alapvető feltételeiről és egyes korlátairól szóló 2008. évi XLVIII. törvény (Grtv.);
- e. A személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól szóló 2005. évi CXXXIII. törvény (Sztv.);
- f. az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény (Eker tv.);
- g. az elektronikus hírközlésről szóló 2003. évi C. törvény - (Ehtv.);
- h. a fogyasztóvédelemről szóló 1997. évi CLV. törvény (Fogyv tv.);
- i. a panaszokról és a közérdekű bejelentésekről szóló 2013. évi CLXV. törvény (Pktv.).

**National Authority for Data Protection and Freedom of Information (NAIH)**

Postal address: 1530 Budapest, Pf.: 5.  
Cím: 1125 Budapest Szilágyi Erzsébet fasor 22/C.  
Phone: 06-1/391-1400  
Fax: 36-1/391-1410  
E-mail address: ugyfelszolgatal@naih.hu  
Website: <http://naih.hu>

(6) As a data subject, in the event of a violation of your rights, you may also file a lawsuit against our Company, in which case the court will act as a matter of priority in the particular case.

**(7) PLEASE NOTE THAT THE PROCESSING OF YOUR DATA IS, OR WILL BE, MANAGED IN ACCORDANCE WITH THE FOLLOWING LAWS:**

- a. The Fundamental Law of Hungary, relevant provisions;
- b. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation / GDPR);
- c. Act CXII of 2011 on Informational Self-Determination and Freedom of Information ("Privacy Act" / Info tv.);
- d. Act XLVIII of 2008 on the Basic Requirements and Certain Restrictions of Commercial Advertising Activities (Grtv.);
- e. Act CXXXIII of 2005 on Security Services and the Activities of Private Investigators ("Security Services Act" / Sztv.);
- f. Act No. CVIII. of 2001 on certain aspects of electronic commerce services and information society services ("E-Commerce Act" / Eker tv.);
- g. Act C of 2003 on electronic communications (Ehtv.);
- h. Act CLV of 1997 on Consumer Protection ("Consumer Protection Act" / Fogyv. tv.);
- i. Act CLXV of 2013 on Complaints and Public Interest Disclosures (Pktv.).



(8) Tájékoztatjuk továbbá, hogy a fentiekben részletezett adatkezeléseink mindenkorú jogosításának biztosítása érdekében rendszeresen felülvizsgáljuk a jelen Szabályzat és valamennyi kapcsolódó Szabályzatunkat. Amennyiben úgy ítélik meg, hogy az aktuális törvényi követelményeknek való megfelelés érdekében azok egyes részeinek módosítása szükséges, úgy megváltoztatjuk azt és átültetjük a módosításokat a jelen Szabályzatba is. A weboldalra látogatóinkat tájékoztatjuk a változásokról egyrészt a [www.hcemm.eu](http://www.hcemm.eu) honlapunkon, valamint kifüggesztjük papír formában is az irodai adminisztrációs feladataink ellátásának otthonát telephelyünkön, a 6723 Szeged, Római körút 21. szám alatt.

(8) We also inform you that we regularly review this Data Processing and Data Security Policy and all related Policies to ensure the legitimacy of our data processing as detailed above. If we deem it necessary to amend certain parts of such policies in order to comply with the current legal requirements, we will change them and transfer the amendments to our Data Processing and Data Security Policy. We inform our visitors about the changes both on our website: [www.hcemm.eu](http://www.hcemm.eu), and by posting them in paper form at our office, 6723 Szeged, Római körút, which hosts our office administration tasks.

## Hatálybalépés

Jelen Szabályzat a kihirdetés napján lép hatályba.

Engedélyezve

A HCEMM Nonprofit Kft. nevében

**HCEMM Nonprofit Kft.**  
6720 Szeged, Dugonics tér 13.  
Th.: 6723 Szeged, Római krt. 21.  
Asz.: 26307383-2-06  
(3.)

Dr. Szabó István, ügyvezető



## Entry into force

This Policy shall enter into force on the day of its publication.

Approved by

on behalf of the HCEMM Non-profit Kft.



Dr. István Szabó, CEO

**HCEMM Nonprofit Kft.**  
6720 Szeged, Dugonics tér 13.  
Th.: 6723 Szeged, Római krt. 21.  
Asz.: 26307383-2-06  
(3.)

