

INTERNAL DATA PROTECTION AND DATA SECURITY POLICY

Content

Article 1 – Contacts of controller.....	3
Article 2 – Definitions	3
Article 3 – General provisions, principles of processing, controller’s record.....	4
Article 4 – Operating of electronic monitoring system (camera system) and access to system.....	6
Article 5 – Data protection system of the company, legal status and duties of the data protection officer, training in connection with data protection	6
Article 6- Data Security Rules	7
Article 7 –Segments of data transfer and processing activities	9
Article 8 – Enforcement of the rights of data subjects.....	13
Article 9 - Revision	16
ARTICLE 10 - Final provisions.....	16

The purpose of the HCEMM Non-profit Kft. (hereinafter referred to as the "Company" or the "Controller") issuing this present Internal Data Protection-and Data Security Policy (hereinafter referred to as the "Policy") is to provide the data subjects information with concise, clear and plain content about all circumstances of the Company's processing activities, in particular about the legal basis, the purpose, the method, the duration of the processing and the rights of data subjects. HCEMM Non-profit Kft. is committed to secure the lawfulness of processing, under which the Company implements appropriate technical and organisational measures for the purpose of ensuring the rights of data subjects and securing the personal data of the data subjects thereby preventing unauthorised access to, alteration of or disclosure of personal data.

HCEMM Non-profit Kft. processes personal data in compliance with the 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) (hereinafter referred to as the "GDPR"), and with the Act CXII of 2011 on the right to information and self-determination and on the freedom of information (hereinafter referred to as the "Privacy Act"), having regard to the guidelines issued by the Chairperson of the National Authority for Data Protection and Freedom as well.

Article 1 – Contacts of controller

1. Name: HCEMM Non-profit Kft.

Registered seat: H-6720 Szeged, Dugonics square 13.

Places of business: H-6726 Szeged, Temesvári boulevard 21.; H-6720 Szeged, Korányi alley 6.; H-6723 Szeged, Római square 21.

Head office of central administration: H-6723 Szeged, Római square 21.

Tax nr.: 26307383-2-06

Website: www.hcemm.eu

2. The present Policy is available at:

https://www.hcemm.eu/wp-content/uploads/2020/08/hcemm_data_protection_policy.pdf

E-mail: office@hcemm.eu

Name and contact information of the Data Protection Officer: Dr. Viktória Papp (gdpr@hcemm.eu)

3. The provisions laid down in this present Policy should be interpreted in harmony with the provisions stipulated in the rest of the regulations of the Company. If regarding the protection of personal data there could be any contradiction between provisions stipulated herein and the provisions stipulated in any other regulations that already have been in force before this present Policy becomes effective, in such case the provisions of this present Policy shall be of governing force.

Article 2 – Definitions

4. The conceptual scheme applied by this present Policy is identical to the definitions set out in Article 4 of the GDPR (definitions) and in Section 3 of the Privacy Act (interpretative provisions).

5. Abbreviations under this present Policy:

- „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);

- **„Privacy Act“** means the Act XCII of 2011 on the Right of Informational Self-Determination and Freedom of Information
- **„NAIH or Authority“** means the Hungarian National Authority for Data Protection and Freedom of Information;
- **„EMBL“** as the **„European Molecular Biology Laboratory“** is 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;
- **„Horizon 2020 framework programme“** is the source of funding that can be obtained, in an international competition, directly from Brussels based on 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;
- **„NRDIO as the National Research, Development and Innovation Office“** purpose is based on Act LXXVI of 2014 on Scientific Research, Development and Innovation is to establish a stable institutional system of governmental coordination and predictable financing of domestic research and development and innovation ensuring efficient, transparent and value-adding use of the available resources.

Article 3 – General provisions, principles of processing, controller's record

Regarding the principles set out in Chapter II. of the GDPR and Chapter II. of the Privacy Act, during the processing of personal data, the Company follows the below provisions:

6. In view of the fact that the right of informational self-determination is a fundamental right provided by the Fundamental Law, in the course of any proceeding, the Company processes data only and exclusively on the basis of the provisions stipulated in the legal rules in force.

7. Personal data may only be processed for a clearly defined, legitimate purpose, to exercise a right and fulfil an obligation in accordance with this present Policy and with the privacy notice and information of processing annexed to this present Policy. At all stages of processing, it must be appropriate to the purpose of the processing, and the collection and handling of data must be fair and lawful. Processing should always correspond with the purpose limitation principle; only such personal data may be processed that is necessary for the realization of the purpose of processing and suitable for the achievement of the purpose. Personal data may be processed by the Company to the minimum extent and for the shortest period necessary for the achievement of the specified and explicit purposes, where it is necessary for the implementation of certain rights and obligations based on the legal basis stated in Article 6-10 of the GDPR and with regard to the principles related to processing of personal data. The purpose of processing must be met at all stages of processing operations, and in case the purpose of processing has ceased, or the processing otherwise violates the law, data should be erased. Erasure of data is the responsibility of the employee of the Company – with the involvement of the Chief Operating Officer and the DPO if necessary – who processes such data. Erasure may be checked by the Chief Operating Officer, the Chief Operating Officer or by the DPO, respectively.

8. Prior to capturing data, the Company in all cases informs the data subject about all the circumstances of the processing, such as in particular the purpose and the legal ground for processing.

9. The employees processing data at the organisational units of the Company and the employees of organisations that are designated by the Company to participate in processing or in any of the operations belonging to processing are obliged to preserve personal data coming to their knowledge as business secret. Persons processing and having access to personal data are obliged to make a **Declaration of Confidentiality** (Annex 1).

10. If a person under the scope of this Policy would gain knowledge of the fact that personal data processed by the Company would be deficient, incomplete or outdated, that person is obliged to rectify same or arrange for its rectification by the employee responsible for data capturing given the fact that during processing the accuracy and completeness of data needs to be ensured as well as the fact that the data is up-to-date – if that is necessary with regard to the purpose of the processing that the data subject may be identifiable only for the time period necessary for the purpose of the processing.

11. The Company, through the DPO, maintains the controller's record of its processing activities in all respects in accordance with Article 30 of the GDPR and with Article 25/E. of the Privacy Act, which includes in particular the follows:

- the name and contact details of the controller and the name and contact details of the joint controller, the controller 's representative and the data protection officer;
- the legal basis or legal grounds, the purpose or purposes of the processing;
- a description of the categories of data subjects and the categories of personal data and the rights of the data subjects;
- in the event of the transfer or planned transfer of personal data, the scope of the recipients of the data transfer;
- the retention period for the different categories of data;
- the general description of the implemented technical and organisational security measures.

The controller's record may be requested upon submitting a written request to the DPO of the Company.

12. The Company's CEO through the DPO keeps a record in order to check measures taken in respect of personal data breaches and in order to keep data subjects informed, which should contain the scope of personal data of the data subject, the scope and the headcount of data subjects concerned by a data breach, date, circumstances, impacts of the data breach and the measures taken in order to prevent incidents, furthermore other data specified in the legal rule requesting processing. The Company informs the organisations and persons concerned by the data breach about the data breach occurred without delay but within 72 hours after becoming aware of the data breach at the latest. The personal data breach should not be notified when it is unlikely to result in a risk to the enforcement of the data subjects' rights. The detailed rules for the handling of data breach and the sample of the register for data breach are regulated by the Company in a separate procedure for the handling of data breach from this present Policy.

13. Data protection obligations applicable to natural or legal persons or organisations without legal personality that are designated by the Company to perform processing activities should be enforced in the service contract concluded with the processor. The Company concludes a data processing contract with the processor as stipulated by the Privacy Act. Annex 4 of the present policy contains further data protection points to be included into the data processing contract. The sample of the data processing contract is annexed to this present Policy (2nd annex).

14. The Company informs the data subjects that, as a general provision, the Company does not process sensitive data, only in exceptional cases strictly under the additional conditions set out in Article 9. of the GDPR. If any of the Company's processing activities necessarily includes processing sensitive data, the Company shall inform in written the data subjects thereof in advance.

Article 4 – Operating of electronic monitoring system (camera system) and access to system

15. The Company's main place of business and the head office of central administration is currently at a rental property located in the Római körút Office Building (H-6723 Szeged, Római square. 21.). The operation of the Office Building, including the professional-technical operation of the equipped cameras and the access system as well, is performed by Római körút Office Building 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. Pictograms inside and outside of the building indicates the placement of the cameras.

16. Both the purpose and the legal basis and all the circumstances of the processing are determined by Római körút Irodaház Kft. which sets out in its 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 and may be requested from the Római körút Irodaház Kft. as well.

17. The Római körút Irodaház Kft. has implemented an access system for which the Római körút Irodaház Kft. is responsible.

18. In addition to the above, those who enter into the area of the Office Building – including the area of the car park – shall comply with the provisions of the Római körút Irodaház Kft.'s House Rules.

19. Questions arising in connection with the processing of personal data related to the electronic surveillance system or the access system should be submitted directly to the Római körút Irodaház Kft. (seat: H-6725 Szeged, Kisfaludy street 3.) using the following e-mail address: romaiirodahaz@gmail.com.

Article 5 – Data protection system of the company, legal status and duties of the data protection officer, training in connection with data protection

20. The CEO of the Company will in due consideration of the specific features of the Company determine the data protection organisation and the scopes of responsibilities and authorities related to such activity.

21. Members of the staff of the Company shall be responsible for the observation of the provisions stipulated in this Policy within their respective scopes of responsibilities.

22. In the course of their work, the members of the staff of the Company ensure that unauthorised individuals will not view personal data and that personal data will be stored and located in such manner that they are not accessible, readable, changeable and/or destroyable by unauthorised individuals.

23. The Company's data protection system is overseen by the CEO through the DPO mandated by the Company in particular with regard the the fact that pursuant to Article 37 (1) (a) of the GDPR, the Company

is required to designate a DPO, and furthermore besides to comply with the legal requirements for the processing of personal data, the Company deemed it important to designate a DPO to ensure the highest possible level of data subject's rights. The name and the contact details of the DPO has been indicated in this present Policy and the NAIH has been informed about the DPO.

24. Legal status of the DPO:

- is directly and exclusively responsible to the managing director and to the Chief Operating Officer;
- may not be instructed in connection with the performance of his/her duties, performs his/her duties alone and independently, may not be dismissed in connection with the performance of his/her duties, shall not be subject to sanctions;
- assists data subjects in all matters relating to the processing of their personal data and the exercise of their rights in connection with the processing;
- in connection with the performance of his / her duties, has the right to access to all personal processing operations of the Company;
- is bound by the obligation of professional secrecy or confidentiality with regard to the performance of his/her duties;

25. Duties of the DPO in relation to data protection:

- assist in securing the rights of the data subject;
- provides information and assistance to all employees of the Company in connection with this present Policy and legal provisions and obligations related to data protection, as well as provide professional advice and monitor the implementation of data protection impact assessments, if necessary to strengthen data protection awareness provides training to the employees if it is necessary;
- keeps the Company's controller record in accordance with Article 30 of the GDPR and the data transfer register up to date, inform the NAIH if it is necessary without delay (within 72 hours at the latest) about any data breach that has occurred;
- checks and may check at all organizational units within the Company whether the data protection processes comply with the provisions of this present Policy and the legal provisions related to data protection;
- cooperates with the NAIH or liaise with the Authority on matters relating to processing, where a question cannot be clearly answered by legal interpretation;
- monitors changes in legislation related to data protection and freedom of information, on the basis of which, if appropriate, initiates amendments to this present Policy.

Article 6- Data Security Rules

6.1 Physical protection

26. In the interest of the security of personal data processed in hard copies, the Company applies in particular the following measures:

- data may be known only by entitled persons, others may not have access to them, also, data may not be revealed for others;
- documents should be placed in a properly lockable, dry room, supplied with fire prevention and security devices;
- documents actually in the course of processing may be accessed by competent persons only;

- if the employee of the Company who is actually engaged in data processing would during the day wish to leave his/her room where data are processed, he/she should place data media in his/her care in a locked place, or should lock the office;
- if paper-based personal data would be digitised, the Company will apply security rules governing the storage of digital documents.

27. When the purpose of the processing of personal data stored on paper has been achieved, the Company takes measures to destroy the hard copies.

6.2 Information technology protection, server security

28. In order to ensure the security of personal data stored on the computer or on the network, the Company applies the provisions set out in the Information Security Policy (hereinafter referred to as the "ISP"), in compliance with which, the Company applies the following measures and warranty elements:

- the computers used during the processing are the property of the Company or the Company has the right of use on them;
- the data on the computer can only be accessed with a valid, personal, identifiable right - at least with a username and password - the Company will ensure the exchange of passwords on a regular basis or in justified cases;
- all computer records with the data are traceably logged;
- the data stored on the network server machine (hereinafter: server) may be accessed only with appropriate authority and only by designated persons
- when the purpose of the processing has been achieved, the deadline for processing has expired, the file containing the data will be irretrievably deleted, the data cannot be recovered again
- the server is stored in a secure location and manner;
- continuously provides virus protection on the personal processing network;
- prevent unauthorized persons from gaining access to the network by using the available computer equipment.

6.3 Privacy-by-design

29. The responsible managers of each department dealing with personal data continuously monitor the compliance with the provisions in connection with data protection especially of this present Policy and its related documents. Prior to the audit the DPO in cooperation with the Chief Operating Officer, shall provide the regional managers with the appropriate professional assistance and the priorities on which basis the audit will be carried out.

30. Each processing operation should be checked as necessary, but at least once a year.

31. The DPO shall inform the CEO in writing about the observations and experience of the audit.

32. Before preparing the information in writing, the DPO shall consult the Chief Operating Officer and the head of each department and make a proposal to the CEO to take the necessary measures.

6.4 Data Protection Impact Assessment

33. If a new process is likely to pose a high risk to the rights and freedoms of natural persons due to its nature, scope, circumstances and purposes, the Company will conduct a data protection impact assessment on how the processing process affects personal data before starting processing.

34. The data protection impact assessment is, as a general rule, carried out by the DPO. If the DPO does not do so, the Company is obliged to seek the professional advice of the DPO.

35. The Company carries out the data protection impact assessment taking into account the criteria described in Annex 3 of this present Policy.

36. If the data protection impact assessment concludes that the processing is likely to involve a high level of risk, the Company will initiate a consultation with the Authority prior to the commencement of the processing.

6.5 Training in connection with data protection

37. The fundamental objective of the Company is that, during their work, its Employees acquaint themselves with and are able to correctly and consistently apply the relevant rules related to processing of personal data, data protection and its policies (especially this present Policy, the ISP, and the procedure for the handling of data breach as well).

38. The Company provides its employees with education and further training on data protection and data security upon entry and, subsequently, annually.

39. During the annual renewal trainings held by the DPO, the new processes and regulations are presented.

Article 7 –Segments of data transfer and processing activities

7.1 Segments of data transfer

40. 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.

41. 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 processing operations will take place. This establishes the regular provision of data to other domestic and foreign resident companies, organisations and institutions, the conditions of which processing shall be set out in the certain cooperation agreement.

42. **Purpose of the processing:** performing the certain cooperation agreement, fulfilling the contract

43. **Scope of data processed:** the name of the legal representative of the company, other personal data given by that person in the contract

44. **Legal basis of the processing:** Article 6 (1) Point b) of the GDPR [performing the contract] in connection with the legal representative of the partner organizations; Article 6 (1) Point f) of the GDPR [legitimate interest pursued by the controller] in connection with the contact person's personal data given in the cooperation agreement, in respect of which the result of the balance interest test may be requested from the DPO in writing (gdpr@hceмм.eu); Article 6 (1) (c) of the GDPR [processing is necessary for compliance with a legal obligation to which the controller is subject].

45. **Storage period:** until the termination of the contract; following the termination of the contract for the enforcement and protection of legal claims arising out of the contract, the Company will keep the personal data provided hereunder as per the general rules of limitation laid down in the Civil Code, and as per the provisions on the preservation of documents in the Accounting Law of Hungary; furthermore taking into account that the operation of the Company is partly financed by European Union fund, partly by governmental budgetary source, the Company is obliged to keep some specific data related to certain contracts until the deadline specified in the relevant grant agreements.

46. **Enforcement of the rights of the data subjects:** set out in the 8th Chapter of this present Policy

7.2 Processing activities

a) Processing related to personal data of applicants applying for positions to be filled and to unsolicited resumes

47. The Company does not use anonymous job advertisements. The Company's selection process of the Company is differentiated depending on whether the position to be filled is a scientific or a non-scientific (HQ) position. With regard to the scientific positions the recruitment process is a complex, multi-round procedure, and all stages of which the Company provides continuous and detailed information to the candidates through its website as well (<https://www.hcemm.eu/core-group-call/>). The Company publishes vacancies for scientific and non-scientific (HQ) positions on its website (<https://www.hcemm.eu/careers/>) or on job advertisement websites. Candidates may apply directly for the positions to be filled on the Company's own website, or it is also possible for those who are interested, to send their CVs directly to the Company's following e-mail address: career@hcemm.eu, even if there are no advertised positions to be filled on the Company's website (unsolicited resumes).

48. With regard to the fact that the HCEMM Non-profit Kft. is a publicly funded company, before the establishment of the employment relationship, during the recruitment procedure, or during the existence of the employment relationship, the Company may require the data subjects to certify their history of integrity, if proof of moral suitability is essential for filling the given position as defined in a sectoral law or if the Company has legitimate interest in doing so. 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. If the Company has a legitimate interest to require from the data subject to proof of moral suitability, in that case before the processing the Company, the Company performs the necessary balance of interest test and if the result of such test establishes that the legitimate interest of the Company outweighs the rights of the data subjects to the protection of personal data, the Company calls on the data subject to proof of moral suitability. The Company requests the moral certificate of good conduct only for presentation.

49. The Company stores the received CV's for the purpose of later use for the period of 1 year from receiving the CV if the candidate prior gives its explicit consent to the processing in order to use the CV later during a new recruitment procedure for a position that becomes vacant later.

50. The Company notifies the applicants about the result of the recruitment procedure regardless that the application succeeds or not. The Company notifies the data subjects of the unsolicited resumes as well. (Annex 4). In connection with processing the personal data of the employee, the Company provides a separate policy.

Conditions of the processing related to personal data of applicants applying for positions to be filled and to unsolicited resumes:

51. Purpose of the processing: to fill the vacant positions, establishment of employment relationship, to conduct the recruitment procedure for a certain vacant position

52. Scope of data processed: name, place and date of birth, mother's name, address, education data, picture, cell number, e-mail address, record about the applicant provided by the employer, other information given by the applicant, other information given on the CV

53. Legal basis of the processing: consent of the data subject given in accordance with Article 6 (1) Point a) of the GDPR; in case of certificate of good conduct: Article 6 (1) Point of the GDPR [legitimate interest of the Company]

54. Storage period: until the recruitment process will be completed or if the applicant gives his/her consent, in that case for one year from the date when the data subject gives her/his consent to store his/her CV in database

55. Method of storage: electronically

56. Enforcement of the rights of the data subjects: set out in the 8th Chapter of this present Policy

b) Data processing relating to procurement procedures reaching or below the procurement value threshold

57. The Company also takes into account the principles of privacy by design and default data protection during public procurements and procurement procedures that do not reach the public procurement threshold. The information of processing in connection with public procurement procedures is provided in Annex 5 of this present Policy. The information of processing in connection with procurement procedures below the public procurement threshold is set out in Annex 6 of this present Policy, which information of such processing is also published on the Company's website.

c) Processing in connection with contracts

58. The Company complies with the data protection provisions set out in the GDPR and in the Privacy Act regards with the concluded contracts as well, due to which when the Company concludes a contract with natural or legal persons or organisations without legal personality where during the performance of such contract other subcontractor does not participate, the processing is carried out by the Company based on the follows:

59. Purpose of the processing: fulfilling the contract

60. Scope of data processed: the name of the legal representative of the company, other personal data given by that person in the contract

61. Legal basis of the processing: Article 6 (1) Point b) of the GDPR [performing the contract]

62. Storage period: until the termination of the contract; following the termination of the contract for the enforcement and protection of legal claims arising out of the contract, the Company will keep the personal data provided hereunder as per the general rules of limitation laid down in the Civil Code, and as per the provisions on the preservation of documents in the Accounting Law of Hungary; furthermore taking into

account that the operation of the Company is partly financed by European Union fund, partly by governmental budgetary source, the Company is obliged to keep some specific data related to certain contracts until the deadline specified in the relevant grant agreements.

63. Storing method: electronically and on paper

64. Enforcement the rights of the data subjects: set out in the 8th Chapter of this present Policy

65. The Company complies with the data protection provisions set out in the GDPR and in the Privacy Act regards with the concluded contracts as well, due to which when the Company concludes a contract with legal persons or organisations without legal personality where during the performance of such contract other subcontractor participates as well, the processing is carried out by the Company based on the follows:

66. Purpose of the processing: fulfilling the contract, and communication with the other party

67. Scope of data processed: the name of the legal representative of the company, other person's data given in the contract

68. Legal basis of the processing: Article 6 (1) Point f) of the GDPR [legitimate interest pursued by the controller] in connection with the contact person's personal data given in the contract, in respect of which the result of the balance interest test may be requested from the DPO in writing (gdpr@hceimm.eu)

69. Storage period: until the fulfilment of the contract

70. Storing method: electronically and on paper

72. Enforcement the rights of the data subjects: set out in the 8th Chapter of this present Policy

d) Online presence, usage of cookies

73. The HCEMM Non-profit Kft. has its own website: <https://www.hceimm.eu>

74. The homepage operated by the Company can be accessed by anyone without revealing his/her identity and giving his/her personal data, also, information can be retrieved from the homepage and the linked sites freely and without restrictions. Meanwhile the homepage gathers non-personal information about its visitors without any restriction. From these pieces of information personal data cannot be retrieved, therefore this is not constituted as data controlling coming under the scope of Privacy Act.

75. Cookie management: Due to the international activities and nature of the Company, as well as the fact that the website can is entirely created in English, in addition to the content on the website individuals can only read the Cookies and privacy policy in English. (<https://www.hceimm.eu/cookies-privacy-policy/>)

76. On its homepage the Company utilises a web analytics service named Google Analytics. Google Analytics applies cookies and text files downloaded on the computer of the visitor of the website, the aim of which is the facilitation of the analysis of the use of the website. Pieces of information generated by the cookies and related to the use of the website (IP-address of the visitor of the website) are transferred to the server of Google located in the United States of America and are stored there. Google does not interconnect information generated by the cookies with other data, therefore, according to the data protection regulation in force it cannot be deemed to be data processing. By way of appropriately setting his/her browser, the visitor of the website can refuse the application of cookies. By virtue of using the website, the visitor of the homepage consents the processing of his/her data in the manner and/or the purpose as discussed above.

Pieces of information so acquired are used by Google for the evaluation of the use of the homepage by data subjects, for analyses, compilation of reports on operations performed on the website, and for delivering other services related to operations performed on the homepage and to internet usage.

Article 8 – Enforcement of the rights of data subjects

8.1 Right to information

77. The data subject may request information on the processing of his / her personal data, as well as request the correction or deletion of his / her personal data at the contact details of the Company, with the exception of the processing ordered by law.

78. The Company is obliged to forward the received application or protest to the head of the organizational unit responsible for processing within three days of receipt.

79. The head of the organizational unit with tasks and competencies shall respond to the request related to the processing of the personal data of the data subject in writing in a comprehensible form no later than 25 days or no later than 15 days in the case of exercising the right to protest.

80. If the assessment of the case is not clear in the exercise of the data subject's rights, the head of the relevant organizational unit may request a resolution from the DPO by sending the case file and his / her position on the case, who shall give his/her opinion within three days.

81. The information shall cover the information specified in Article 15 (1) of the GDPR, provided that the information of the data subject cannot be refused by law. The Company shall take appropriate measures to provide the data subject with all information concerning the processing of personal data referred to in Articles 13 and 14 of the GDPR and shall provide each information in a concise, transparent, comprehensible and easily accessible form, in a clear and comprehensible manner in accordance with Articles 15 to 22 and Article 34 of the GDPR. The information shall be provided in writing or by other means, including, where appropriate, by electronic means. Oral information may be provided at the request of the data subject, provided that the identity of the data subject has been otherwise established.

82. The information is, in principle, free of charge, the Company may charge a fee only in the case specified in Article 12 (5) (a) of the GDPR.

83. The Company shall reject the application only for the reasons specified in Article 12 (5) (b) of the GDPR, and this may only be done in writing, with due justification and appropriate information.

8.2 Right to rectification, cancellation (forgetting)

84. Inaccurate data shall be corrected by the head of the department processing the data, if the necessary data and authentic instruments proving them are available and shall take steps to delete the processed personal data if the reasons set out in Article 17 of the GDPR exist.

85. The data subject shall have the right, at his/her request, to have the personal data concerning him/her deleted without undue delay and the Company shall delete the personal data concerning him/her without undue delay, in particular if one of the following reasons exists:

- personal data are no longer required for the purpose for which they were collected or otherwise processed;
- the data subject withdraws his or her consent and there is no other legal basis for the processing;

- the data subject objects to the processing and there is no overriding legitimate reason for the processing or the data subject objects to the processing for the direct acquisition of business;
- personal data have been processed unlawfully;
- personal data were collected in connection with the provision of information society services to children under the age of 16;
- if the Controller has disclosed the personal data and the personal data are no longer needed for the purpose for which they were collected or otherwise processed, it shall delete it and take reasonable steps, taking into account the available technology and implementation costs, including technical measures to inform the controllers that the data subject has requested the deletion of links to the personal data in question or of a copy or duplicate of such personal data.

8.3 Protest against the processing of personal data

86. The data subject has the right to object to the processing of his / her personal data at any time by means of a statement to the Company, in particular if the processing or transfer of personal data is necessary solely to fulfil a legal obligation to the Controller or the legitimate interests of the Controller, in the case of mandatory processing or if the use or transfer of personal data is for the purpose of direct business acquisition, public opinion polling or scientific research; and in other cases specified by law.

87. For the duration of the examination of the data subject's objection to the processing of personal data, but for a maximum of 5 days, the controller shall suspend the processing, examine the grounds for the objection and make a decision, informing the applicant in accordance with Article 19 of the GDPR.

88. If the objection is justified, the controller shall act in accordance with Article 21 of the GDPR.

89. If the Controller establishes that the protest of the data subject is justified, then Controller terminates the processing of data, including further data collection and transmission, blocks the data and notifies about the protest and the action taken on it all those whom the personal data affected and those to whom the protest have previously been transmitted and who are obliged to take measures to enforce the right to protest.

90. If the data subject does not agree with the decision of the Controller, or if the Controller fails to meet the deadline for replying, the data subject may apply to a court within 30 days from the notification of the decision or the last day of the deadline.

91. If the data subject does not receive the data necessary for the exercise of the data subject's right due to the data subject's protest, he / she may challenge the Controller in court in 15 days from the service of the notification in order to obtain the data. The Controller may also sue the data subject.

92. If the Controller fails to notify, the Recipient may request information from the Controller regarding the circumstances related to the failure of the data transfer, which the Controller is obliged to provide within 8 days after the delivery of the Recipient's request. In the event of a request for information, the data recipient may challenge the Controller in court within 15 days of the provision of the information, but no later than within the open deadline. The Controller may also sue the data subject.

93. The Controller may not delete the data of the data subject if the processing has been ordered by law. However, the data may not be transferred to the data recipient if the controller has agreed to the protest or the court has established the legitimacy of the protest.

94. If the assessment of the case is unclear in the exercise of the data subject's rights, the head of the department handling the data may request a resolution from the DPO by sending the case file and his / her position on the case, who shall comply with it within three days.

8.4 Right to restrict processing

95. The data subject has the right to have the processing at the Company restricted if
- the data subject disputes the accuracy of the personal data (in this case, the restriction applies to the period of time that allows the Company to verify the accuracy of the personal data);
 - the processing is unlawful and the data subject opposes the deletion of the data and instead requests that their use be restricted;
 - the Company no longer needs personal data for the purpose of processing, but the data subject requests it in order to submit, enforce or protect legal claims;
 - the processing is necessary for the performance of a public interest task or the processing is necessary for the legitimate interests of the Company or a third party and the data subject objects to the processing for these purposes (in this case the restriction applies until the Company is take precedence over the legitimate reasons of the data subject).

96. Restriction of processing means that the Company does not process the personal data affected by the restriction, except for storage, or only to the extent to which the data subject has consented, or the Company may, in the absence of such consent, handle the data necessary to protect the rights of another natural or legal person or in the overriding public interest of the Union or of a Member State of the European Union. The Company informs the data subject in advance about the lifting of the processing restriction.

8.5 The right to data portability

97. In the course of the processing activities of the Company recorded in this processing prospectus, no processing is carried out that would require the provision of data portability.

8.6 Automated decisions making in individual cases, including profiling

98. Automated decision-making does not take place during the Controller's processing.

8.7 Right to compensation for damage caused by unlawful processing

99. The controller shall also reimburse the damage caused to others by the unlawful processing of the data subject's data or the violation of data security requirements, as well as the damages caused by the personal data violation caused by it or the data processor used by it. The controller shall be released from liability for the damage caused and the obligation to pay damages if he proves that the damage or the violation of the data subject's personal rights was caused by an unavoidable cause outside the scope of processing. Likewise, it does not compensate for damage if it was caused by the intentional or grossly negligent conduct of the injured party.

8.8 Right to legal remedy

100. The relevant legal remedy or complaint may be addressed to the data protection officer of the Company (Dr. Viktória Papp; gdpr@hceмм.eu) directly or, at his/her option, to the National Data Protection and Freedom of Information Authority (1055 Budapest, Falk Miksa utca 9-11, mailing address: 1363 Budapest, Pf. 9.) or to the court having jurisdiction over the place of residence or stay. In order to enforce the right to a judicial remedy, the data subject may, in the context of data processing operations falling within the scope of the controller's activities, take legal action against the controller if he considers that the controller or the controller acting on his behalf in breach of the rules laid down in law or in a binding act of the European Union. The court is acting bypassing other issues in such case.

Article 9 - Revision

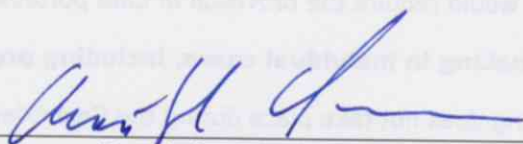
101 The Company regularly review this present Policy and all related Policies to ensure the legitimacy of the processing of personal data as detailed above. If the Company deems it necessary to amend certain parts of such policies in order to comply with the current legal requirements, the Company will change them and transfer the amendments to this present Policy as well. The Company informs the visitors of its website about the modifications both on its website: www.hcemm.eu and by posting them in paper form at the Office (address: H-6723 Szeged, Római krt. 21.) as well.

ARTICLE 10 - Final provisions

102. In the event of a change in legislation, the Company's regulations shall be reviewed, and the necessary amendments shall be implemented within the time limit prescribed therein, but not later than within 90 days.

103. The updating of the rules of the Company and the preparation of the necessary amendments shall be approved by the HCEMM DG/CEO of the Company.

104. The Policy shall enter into force on **1 September 2021**.



Dr. Christoph W. Sensen
HCEMM Director General/Chief Executive Officer

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