DATA MANAGEMENT AND PRIVACY POLICY

Semmelweis Premium Medical Care Services and Consulting Ltd. (registered office: 1085 Budapest, Üllői út 26., hereinafter referred to as: Service Provider, or Data Controller, or Company), acknowledges the content of this legal notice as binding on itself, and at the same time undertakes to ensure that all data processing related to its activities complies with the requirements set out in this regulation and in the applicable national legislation and legal acts of the European Union.

The data management and data protection regulations of Semmelweis Premium Medical Care Services and Consulting Ltd. (hereinafter referred to as the Regulations) are continuously available at www.semmelweispremium.hu.

Semmelweis Premium Medical Care Services and Consulting Ltd. reserves the right to change the Regulations at any time, with the proviso that it notifies its clients and partners about the changes 15 days in advance by publishing them on the website www.semmelweispremium.hu.

Semmelweis Premium Medical Care Services and Consulting Ltd. is committed to protecting the personal data of its clients and partners and considers it particularly important to respect its clients' right to informational self-determination.

Semmelweis Premium Medical Care Services and Consulting Ltd. treats personal data confidentially and takes all security, technical and organizational measures to guarantee the security of the data.

This privacy policy will enter into force .

Róbert Kovács

Managing director

I. INTRODUCTION

Definitions

Data processing: all data processing operations performed by a data processor acting on behalf of or on the instructions of the data controller.

Data processor: a natural or legal person or an organisation without legal personality who processes personal data on behalf of or on the instructions of the data controller, within the framework and under the conditions specified by law or in a binding legal act of the European Union.

Data management: any operation or set of operations performed on data, regardless of the procedure used, in particular collection, recording, organisation, storage, alteration, use, consultation, transmission, disclosure, alignment or combination, blocking, erasure and destruction, as well as preventing further use of the data, taking photographs, audio or video recordings and recording physical characteristics suitable for identifying a person (e.g. fingerprints or palm prints, DNA samples, iris images);

Data marking: providing data with an identification mark for the purpose of distinguishing it.

Data destruction: complete physical destruction of the data medium containing the data

Data transfer: making data available to a specific third party

Data erasure: making data unrecognizable in such a way that its recovery is no longer possible

Data blocking: providing data with an identification mark to limit its further processing permanently or for a specified period of time

Data breach: a breach of security that results in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to, personal data transmitted, stored, or otherwise processed.

Healthcare provider: the treating physician, the healthcare professional, any other person performing activities related to the medical treatment of the person concerned, the pharmacist

Health data: personal data relating to the physical or mental health of a natural person, including data relating to health services provided to the natural person which contain information about the health status of the natural person

Health documentation: a record, register or any other recorded data containing health and personal identification data that has come to the attention of the patient care provider during medical treatment, regardless of its medium or form

Consent: a voluntary, definite and unambiguous and based on the proper indication of the person concerned based, by which the person concerned, or by other clearly expressed way they declare their consent to managing personal data relating to them

Act CLIV of 1997 on Health:

medical treatment: any activity aimed at the direct examination, treatment, care, medical rehabilitation of the person concerned, and the processing of the test materials of the person concerned for the purpose of preserving health, preventing, early detecting, diagnosing, curing diseases, maintaining or improving the deterioration of the condition resulting from the disease, including the provision of medicines, medical aids, spa services, rescue and patient transport, and obstetric care;

Info Act: Act CXII of 2011 on the right to informational self-determination and freedom of information

Treating physician: treating physician pursuant to Section 3(b) of Act CLIV of 1997 on healthcare

Close relative: spouse, direct relative, adopted, step- and foster child, adopter, step- and foster parent, sibling and partner

Disclosure: making data available to anyone

Registration system: a file of personal data structured in any way – centralized, decentralized or according to functional or geographical aspects – which is accessible based on specific criteria

Medical secret: health and personal identification data that the data controller has become aware of during medical treatment, as well as other data related to necessary or ongoing or completed medical treatment, as well as other data learned in connection with medical treatment

Profiling: any managing of personal data – by automated means – intended to evaluate, analyse or predict personal characteristics of the person concerned, characteristics relating to their performance at work, economic situation, health, personal preferences or interests, reliability, behaviour, location or movements

Urgent need: such a sudden change in health status that, in the absence of immediate health care, would put the person concerned in immediate danger of death or cause serious or permanent damage to health

Personal data: any information relating to the person concerned

Objection: a statement by the person concerned objecting to the processing of their personal data and requesting the termination of the processing or the deletion of the processed data.

II. SCOPE OF PERSONAL DATA, PURPOSE, TITLE AND DURATION OF DATA PROCESSING

1. The data processing of the activities of Semmelweis Premium Medical Care Servises and Consulting Ltd.. is based on the voluntary consent of the person concerned or on legal authorization. In the case of data processing based on voluntary consent, people concerned may withdraw this consent at any stage of data processing. In certain cases, the processing, storage and transmission of a range of data provided is mandatory by law. If the person concerned does not provide their own personal data, the person concerned is obliged to obtain the person's concerned consent.

2. The basic principles of data management are in line with the applicable data protection legislation, in particular the following:
   a. Act CXII of 2011 - on the right to informational self-determination and freedom of information (InfoAct);
   b. Regulation (EU) 2016/679 of the European Parliament and of the Council (27 April 2016) - on the protection of natural persons regarding the processing of personal data and on the free movement of such data, and repealing Regulation 95/46/EC (General Data Protection Regulation, GDPR);
   c. Act V of 2013 - on the Civil Code (CC);
   d. Act C of 2000 - on accounting (Accounting Act);
   e. Act XLVII of 1997 on the protection of health and related personal data
   f. Act CLIV of 1997 Act on Health Care (hereinafter referred to as the Health Care Act);
   g. 62/1997. (XII.21.) NM Decree on Certain Issues of the Processing of Health Care and Related Personal Data (hereinafter referred to as: R.);
   h. Act C. of 2000 on Accounting (hereinafter referred to as: AAct.);

<u>Scope of processed data</u>

3. The condition for using the services provided by the Service Provider is the conclusion of a written Service Contract between the Service Provider and the patients, with which the patient simultaneously declares their consent to the processing of the data provided by them.

4. The Service Provider processes the following data in the context of providing healthcare services:
   a. patient's personal identification data (family and first name, maiden name, gender, place and date of birth, mother's maiden family and first name, place of residence, place of stay, National Health Service number (TAJ number), citizenship, native language, mailing address, telephone number, e-mail address, tax identification number, student status, name and address of higher education institution, data recorded in the service contract);
   b. in the case of care financed by an insurance company, the details of the insurance company/insurance

c. in the case of care financed by a health fund, the data of the health fund
d. in the case of a competent patient, the name, address and contact details of the person to be notified
e. in the case of a minor or a patient under guardianship that partially or completely limits their capacity to act, the name, address and contact details of the legal representative
f. medical history
g. the test result
h. test results that form the basis for the diagnosis and treatment plan, and the date of the tests
i. the name of the disease defining the treatment, the underlying disease, concomitant diseases and complications
j. other diseases that do not directly justify the treatment, or the name of the risk factors
the time of the interventions performed and their results
k. drugs and other therapy and its results
l. data relating to the patient's drug hypersensitivity
m. the content of the information provided to the patient or other person entitled to get the information
n. the patient's consent to healthcare is required based on the patient's right to self-determination
o. the patient can refuse healthcare under the conditions set out in the Health Act, the fact and date of this refusal
all other data and facts that may have an impact on the patient's recovery.

5. Purpose of data processing:
a. promoting the preservation, improvement and maintenance of health
b. facilitating the effective medical treatment activities of the patient care provider, including professional supervision activities
c. monitoring the health status of the person concerned
d. taking necessary measures in the interests of public health, public hygiene and epidemiological surveillance
e. enforcing patients' rights
f. provision of health services
g. distinguishing between the clients
h. fulfilment and execution of the service contract concluded between the data controller and the client, provision of the service undertaken based on the contract
i. confirmation of obligations and rights related to the contract
j. enforcement, collection and sale of any claims that may arise in connection with the contract
k. profiling
l. keeping in touch
m. follow up of the services used

n. fulfilment of the provisions of Section 4(2) of the Primary Health Care Act
o. marketing inquiry

6. Legal basis of data processing
   a. regarding the points a)-e) of the 5. §- of Primary Health Care Act
   b. regarding the points f)-o), the person's concerned voluntary consent (Article 6 (1) (b) of the GDPR).

7. Possible consequences of failure to provide data: failure to provide healthcare services. Deadline for cancellation of data

8. Health documentation must be kept for at least 30 years from the date of data collection, and the final report for at least 50 years. By way of exception, images taken using diagnostic imaging procedures must be kept for 10 years from the date of their creation, and the report prepared based the image must be kept for 30 years from the date of the creation of the image.

9. Employment data must be kept for 50 years from the termination of the person's concerned employment.

10. The data necessary to fulfil the obligation set out in Sections (1) and (2) of Section 169 of the Accounting Act must be kept for at least 8 years.

11. Data not mentioned above must be deleted within 60 days of reception of the person's concerned request for cancellation.

<u>Data Protection Impact Assessment</u>

12. A data security risk assessment must be carried out for all high-risk data processing.

13. Risk analysis should be carried out regularly, before the introduction of each new process.

14. The opinion of the data protection officer must always be sought on the process and results of the impact assessment.

15. The impact assessment must include:
   a. a description of the planned data processing operations,
   b. a description of the purposes of data processing
   c. in the case of specific purposes, the examination of the necessity and proportionality of data processing operations,
   d. the investigation concerning the rights of the person concerned
   e. presentation of measures aiming to manage risks

III. USE OF SERVICES PROVIDED BY SEMMELWEIS PREMIUM LTD

Recording patient's data

1. In the company patient care is done through an appointment system. the patient's personal and the health data necessary for the examination are recorded in a medical system, either on the server owned by the Company or in an IT system of the subcontractor under contract with Semmelweis Premium Medical Care Services and Consulting Ltd.

2. Handling medical documentation is the responsibility of the attending physician. Documentation is done in the IT system (MedSol) operated by Semmelweis University, in a module created and separated for this purpose.

3. After the completion of the medication, the patient receives a copy of the medical documentation (test results, outpatient medical report, final report). After the medication, the patient, or their close relative or authorized representative - upon request - can access the patient's documentation in the manner regulated below and can receive a copy of it.

4. The fee for issuing a copy is 300 HUF + VAT administration cost, and 25 HUF + VAT copying cost per page. Electronic copying is also possible (e.g. scanning), in which case only an administration cost may be charged. Issuance of a copy of the patient documentation upon request, is the right to get familiarized with the health documentation

5. The patient has the right to access the data regarding them in the medical documentation and to request information about their medical data. When accessing medical documentation, it must be considered that the information must be provided in a careful and gradual manner, taking into account the patient's circumstances.

6. The patient has the right to:
   a. to learn about the health data relating to them
   b. to review their medical documentation
   c. to make an extract/copy of their health documentation and obtain one at their cost
   d. to receive a summary or abstract written opinion on their health data for a justified purpose - at their cost
   e. to receive information about the processing of their data
   f. to receive a final report in cases prescribed by law.

7. Right to knowledge and access
   a. during the period of the person's concerned medication, the person authorised by them in writing

b. after the end of the treatment of the person concerned, it is granted to the person authorized by them in a private document with full evidentiary force.

During the life of the patient or after his death, the spouse, lineal relative, sibling and life partner of the person concerned are also entitled to exercise the right of access and inspection, upon written request, if

a. the health data is necessary for the purpose of
aa) identifying a cause affecting the life and health of the spouse, blood relative, sibling, or life partner, as well as their descendants, or

ab) providing health care to the persons referred to in point aa), and

b. It is not possible to access or draw conclusions about the health data in any other way. In the cases referred to in this point, only that health data can be accessed which directly related to the reasons indicated.

8. In the event of the death of the person concerned - unless otherwise previously provided - their legal representative, close relative and heir are entitled to learn about the health data related to or that can be linked to the cause of death, as well as to the medical treatment prior to death, to inspect the medical documentation and to receive a copy of it. The entitlement must be proved with a document. The copy(s) may only be issued based on an original, fully probative private document containing a request. The original copy of the request must be kept attached to the case file (medical record).

9. In the case of issuing health documentation, the requested documents must be issued as recorded in the medical system. The data protection officer is responsible for issuing the documents. The fact of issuance must be recorded in the documentation and in a separate register. Prior to issuance, the recipient must verify their identity or authorization. The fact of verification must be recorded along with the recipient's personal data and ID card number. If another authorized person requests the documentation, the authorization document must also be attached to the patient documentation.

10. The release of health documentation can only happen with the permission of the managing director in the following cases:
    a. Upon request of the police or other authorities
    b. Upon request of a lawyer
    c. Inquiry regarding a claim for compensation in connection with the treatment.

11. If the medical documentation prepared about the patient also contains data concerning the right to privacy of another person, the right to inspect and issue a copy may only be exercised with respect to the part relating to the patient.

12. A competent patient can make a declaration in a public document, a private document with full probative value or - in the case of illiteracy - in the presence of two witnesses.

    a. can name the competent person who is entitled to exercise the right of consent or refusal on their behalf, or who must be informed
    b. with or without specifying the person specified in point a), any of the people named in points 12-13 can be excluded from exercising the right of consent and refusal on their behalf or from getting information.

13. If the patient is uncapable and there is no authorized person to make the above-mentioned declaration, the following people are entitled to exercise the right of consent and refusal within the limits set out in the above point - considering the written in point 12 - in the order indicated:
    a. the patient's legal representative
    b. failing this, a capable person living in the same household as the patient
        i. spouse or partner
        ii. failing this, their child
        iii. failing this, their parent
        iv. failing this, their sibling
        v. failing this, their grandparent
        vi. failing this, their grandchild
    c. in the absence of a relative specified in point b), a person who is not living in the same household as the patient and can act
        i. child
        ii. failing this, their parent
        iii. failing this, their child
        iv. failing this, their grandparent
        v. failing this, their grandchild

14. The right to access the documentation of a person referred to in Section 16 (1) and (2) of the Health Act, a minor with limited legal capacity and a person whose legal capacity is partially limited in exercising rights related to healthcare shall be granted to the patient, the person named in the power of attorney, or, in the absence of such a person, the legal representative.

15. In case of urgent need, all health and personal identification data known to the treating physician and related to the medical treatment can be transmitted without the consent of the person concerned.

Protection of medical confidentiality

16. The service provider and any other person in an employment or other legal relationship with the service provider are bound by obligation of confidentiality without time limit regarding the data related to the patient's health condition and other data that they have

come to know in connection with their work. The obligation of confidentiality is independent of the way in which the data was obtained. The obligation of confidentiality therefore binds not only the treating physician and the specialists, but also all employees of the service provider. The service provider - except for the forensic medical expert - is also bound by the obligation of confidentiality towards the patient's care provider who did not co-operate in the patient's medical treatment, unless the data is necessary for the further medical treatment of the person being treated. The patient may grant exemption from the obligation of confidentiality in writing, or by a statutory data provision obligation, as well as by the transfer of data to the people specified in this data protection information, to the extent of the data they process.

Transfer of data to third parties

17. Upon written request from the following authorities, the treating physician shall provide the requesting authority with the personal identification data of the person's concerned health care documentation and data can be handled based on the law by the requesting authority and necessary for identification. In the request must indicated the health care and personal identification data that the requesting body wishes to obtain, as well as the purpose of the data processing. The requesting bodies can be the following:
    a. in criminal cases, the investigating authority, the prosecutor's office, the court, the forensic expert, in civil litigation and non-litigation cases, and in administrative cases, the administrative authority, the prosecutor's office, the court, the forensic expert
    b. authorities conducting the procedure during a misdemeanour procedure
    c. in the case of potential conscripts, the office of the capital and county government offices, the military administrative and central data processing body of the Hungarian Defence Forces, and the military medical fitness assessment committee
    d. the national security services, to perform the tasks specified in Act CXXV of 1995 on National Security Services, within the scope of the authorization granted therein
    e. the military administrative and central data processing body of the Hungarian Defence Forces, for the purpose of calling up trained reservists for military duty in peacetime and for the rapid and differentiated call-up of trained reservists, within the scope specified in the Act on National Defence and the Hungarian Defence Forces
    f. the authority and competence to conduct the procedure during an ongoing ethical procedure against a healthcare labour
    g. bodies performing internal crime prevention and crime detection tasks specified in the Police Act, as well as bodies combating terrorism, to perform the tasks specified in the Act, within the scope of the authorization granted therein
    h. during the autopsy, the doctor conducting the post-mortem examination.

18. The request can only be fulfilled if it contains the exact purpose of the data processing and the scope of the requested data.

19. When treating the data subject for the first time, if the data subject has suffered an injury that can be healed for more than 8 days and the injury is likely to be the result of a crime,

the treating physician shall immediately report the person's concerned personal identification data to the police and inform the person concerned thereof.

20. When providing medical care to a minor for the first time, the doctor of the Company is obliged to immediately notify the child welfare service competent for the company's location if:
    a. it is presumed that the child's injury or illness is the result of abuse or neglect
    b. During the medical treatment it becomes aware of circumstances indicating abuse or neglect of the child
21. For data transfer specified in the above points the consent of the person concerned, or the person entitled to access the data is not required

22. Health and personal identification data for the purpose of administrative procedures or the institutional placement and care of the person concerned can be transferred if this is necessary for the enforcement of the person's concerned rights or the fulfilment of their obligations.

23. If the health data of the person concerned also affect another person, the written consent of this third person (legal representative) must be obtained for the transfer of health and personal identification data. Consent is not required if:
    a. if it is probable or confirmed that the person concerned is infected with a pathogen of a disease listed in Annex 1 of the Primary Health Care Act, or suffers from infectious poisoning or an infectious disease, unless the person concerned wishes to participate in an HIV screening test without revealing their identity in advance
    b. if it is necessary to carry out the screening and suitability tests listed in Annex 2 of the Primary Health Care Act
    c. in case of acute poisoning
    d. if it is likely that the person concerned suffers from an occupational disease as defined in Annex 3 of the Primary Health Care Act
    e. if the provision of data is necessary for the medical treatment, preservation or protection of the health of the fetus or minor child
    f. if the competent authority has ordered the investigation for the purpose of law enforcement, crime prevention, or during prosecution, court proceedings, or administrative or misdemeanour proceedings
    g. if the provision of data is necessary for the purpose of control pursuant to the Act on National Security Services
    h. the provision of data is necessary for statistical reasons.

24. The person concerned (their legal representative) is obliged to provide their health and personal identification data upon the Company's request:
    a. if it is probable or confirmed that they are infected with a pathogen of a disease listed in Annex 1 of the Primary Health Care Act, or suffers from an infectious poisoning or infectious disease, except for participation in an anonymous HIV screening test

b. if it is necessary to carry out the screening and suitability tests listed in Annex 2 to the Primary Health Care Act
c. in case of acute poisoning
d. if it is likely that the person concerned suffers from an occupational disease as defined in Annex 3 to the Primary Health Care Act
e. if the provision of data is necessary for the medical treatment, preservation or protection of the health of the fetus or minor child
f. if the competent authority has ordered the investigation for the purpose of law enforcement, crime prevention, or during prosecution, court proceedings, or administrative or misdemeanour proceedings
g. if the provision of data is necessary for the purpose of control pursuant to the Act on National Security Services

25. The Company shall immediately forward to the health administration authority the health and personal identification data obtained during the data collection if it detects or suspects an infectious disease listed in point A) of Annex 1 of the Primary Act.

26. In the event of an infectious disease not listed in Annex 1 of the Primary Act or in the event of a disease listed in point B) of Annex 1, the healthcare provider may report only the health data to the health state administrative authority without personal identification data. The health state administrative authority may request the personal identification data of the person concerned, citing public health or epidemiological interests - with the exception of HIV-infected and AIDS patients examined within the framework of an anonymous screening test.

27. In the case of live birth and death, the health and personal identification data of the person born alive or deceased must be transferred to the Central Statistical Office through the registrar competent for the place of birth or death - for the purpose of monitoring the health status of the person concerned. During the reporting obligation to be fulfilled for the purpose of registering events related to birth or death, the healthcare provider may learn and forward the personal identification data of the child's parents in the case of live birth, and of the surviving spouse or registered partner in the case of death.

28. Upon the service provider's request containing the contact code indicated in the patient documentation, the health insurance body shall immediately provide information electronically about the data stored in the central implant register, including a contact code, regarding the implant-related intervention previously performed on the person treated by the Company.

29. In the case of care financed by an insurance company, the health documentation will be handed over to the relevant insurance company; if consent is refused, the medication cannot be carried out.

Data processors

30. To provide services, Semmelweis Premium Medical Care Services and Consulting Ltd. uses data processors, which are included in Annex 1.

31. Possible consequences of failure to provide data: failure to provide healthcare services.

People present during the treatment

32. During medical treatment, the treating physician and other people involved in patient care may be present, as well as those whose presence the patient has consented to.

33. Without the consent of the person concerned, the following people may be present, while respecting the human rights and dignity of the person concerned:
    a. another person, if the medical treatment regimen requires simultaneous care of several patients
    b. a professional member of the police force, if the medical treatment is provided to a detained person
    c. a member of the penitentiary organization in a service relationship, if the medical treatment is provided to a person serving a sentence involving deprivation of liberty in a penitentiary hospital, and this is necessary for the safety of the patient care provider performing the treatment or to prevent escape
    d. a professional member of the police or a member of the penitentiary organization in a service relationship, if the patient's personal safety justifies this in the interest of law enforcement and the patient is unable to make a statement.

34. In addition to the people specified in the previous point, the following may be present without the consent of the person concerned:
    a. who previously treated the person concerned for that specific illness
    b. to whom the managing director or the data protection officer has given permission for professional scientific purposes, unless the person concerned has expressly objected to this.

35. For healthcare professional training, a doctor, medical student, healthcare professional, a student at a healthcare college, healthcare vocational school or healthcare vocational secondary school may be present during the treatment with the consent of the person concerned (their legal representative).

36. The patient's human rights and dignity must also be respected in this case.

37. The person receiving medical treatment may also give consent orally to the treating physician.

Logging of the www.semmelweispremium.hu server

38. When visiting the website www.semmelweispremium.hu, the web server does not record user data.

Cookie management of the website www.semmelweispremium.hu

39. To provide customized service, the service provider places a small data package, called a cookie, on the user's computer and reads it back during the subsequent visit. If the browser sends back a previously saved cookie, the service provider managing the cookie can connect the user's current visit with previous ones, but only regarding its own content.

40. The purpose of data processing is to identify and distinguish users from each other, to identify the current work session of users, to store the data provided during it, to prevent data loss, to identify and track users, and to perform web analytics measurements.

41. Legal basis for data processing: consent of the person concerned.

42. The scope of the data processed: identification number, date, time, and the previously visited page. Duration of data processing: thirty minutes.

43. The user can delete the cookie from their computer or disable the use of cookies in their browser. Cookies are usually managed in the Tools/Settings menu of browsers under the Privacy/History/Personal settings menu, cookie or tracking.

44. Possible consequences of failure to provide data: incomplete availability of website services, inaccuracy of analytical measurements.

Customer correspondence of Semmelweis Premium Medical Care Servises and Consulting Ltd..

45. If you would like to contact our Company with general information, you can contact the data controller using the contact details provided in this information or on the website. Semmelweis Premium Ltd. deletes all e-mails received by it, together with the sender's name, e-mail address, date, time and other personal data provided in the message, a year after the data was disclosed.

Other data processing

46. A CCTV system may operate in buildings used for the provision of healthcare, information on which is contained in Annex 2 to these regulations.

47. We will provide information on data processing not listed in this information when the data is collected. We inform our clients that the court, the prosecutor, the investigating authority, the misdemeanour authority, the administrative authority, the National Data Protection and Freedom of Information Authority, the Hungarian National Bank, the

National Security Service, or other bodies authorized by law may contact the data controller to provide information, communicate or transfer data, or make documents available. Semmelweis Premium Ltd. will only provide the authorities with personal data to the extent and insofar as the authority has specified the precise purpose and scope of the data, which is necessary to achieve the purpose of the request.

IV. EMPLOYMENT-RELATED DATA PROCESSING

Labour and personnel records

1. Only such data can be requested and recorded from employees, and only such medical fitness examinations may be performed, that are necessary for the establishment, maintenance and termination of employment, or for the provision of social welfare benefits, and that do not violate the personal rights of the employee.

2. The Company processes the following employee data for the purpose of establishing, fulfilling or terminating an employment relationship to enforce the legitimate interests of the employer (Article 6 (1) paragraph f) of the Regulation):
   name, birth name, date of birth, mother's maiden name, address, citizenship, tax identification number, National Health Service number, pensioner registration number (in the case of a retired employee), telephone number, e-mail address, identity card number, official ID number proving address, bank account number, online identifier (if any), start and end date of employment, job title, copy of educational qualification, professional qualification, photograph, CV, amount of salary, data related to salary payment and other benefits, debt to be deducted from the employee's salary based on a final decision or law or written consent, and the entitlement to this, evaluation of the employee's work, method of termination of employment, reasons, depending on the job title, certificate of good conduct, summary of job suitability tests, in the case of private pension fund and voluntary insurance fund membership, name of the fund, identification number and the employee's membership number, passport number in the case of a foreign employee; the name and number of the document certifying the right to work, data recorded in the records of accidents affecting the employee; data necessary for the use of welfare services and commercial accommodation; data recorded by the camera and access control system used by the Company for security and property protection purposes, and by location systems.

3. The employer processes data regarding illness and trade union membership only for the purpose of fulfilling the rights or obligations specified in the Labour Code.

4. Addressee of personal data: the employer's manager, the person exercising employer authority, the Company's employees and data processors performing labour-related tasks.

5. Only the personal data of management employees can be transferred to the owners of the Company.

6. Before starting data processing, the person concerned must be informed that the data processing is based on the Labour Code and the enforcement of the employer's legitimate interests.

7. The employer shall inform the employee about the processing of their personal data and personal rights by providing a leaflet at the same time as concluding the employment contract.

Data processing related to aptitude tests

8. Only such aptitude tests can be applied to an employee that are prescribed by a rule relating to the employment or which are necessary for exercising a right or the fulfilment of an obligation specified in a rule relating to the employment. Before the test, employees must be informed in detail, among other things, about the skills and abilities to be assessed in the aptitude test and the means and methods used to carry out the test. If a law prescribes the performance of the test, employees must be informed of the title of the law and the exact location of the law.

9. The employer can Make employees complete test forms aimed at work aptitude and preparedness both before and during the employment.

10. A test sheet suitable for researching psychological or personality traits and clearly related to employment, and in order to more efficiently manage and organize work processes can only be completed by a larger group of employees if the data revealed during the analysis cannot be linked to specific employees, i.e. the data is processed anonymously.

11. Scope of personal data that can be processed: the fact of suitability for the job and the necessary conditions for this.

12. Legal basis for data processing: legitimate interest of the employer.

13. Purpose of processing personal data: establishing and maintaining an employment, performing the job.

14. Recipients and categories of recipients of personal data: the results of the examination may be known to the examined employees and the specialist conducting the examination. The employer can only receive information on whether the examined person is suitable for the job or not, and what conditions must be provided for this. However, the employer may not learn the details of the examination or its full documentation.

15. Duration of processing of personal data: 3 years after termination of employment.

Data management of the employees applying for employment, applications, CVs

16. The scope of personal data that can be processed: the person's name, date and place of birth, mother's name, address, qualification, photo, telephone number, e-mail address, employer's note about the applicant (if any).

17. The purpose of processing personal data: application, evaluation of applications, conclusion of an employment contract with the selected candidate. The person concerned must be informed if the employer has not selected them for that position.

18. Legal basis for data processing: consent of the person concerned.

19. Recipients of personal data and categories of recipients: the Company's manager and leader with employer's authority, employees performing personnel duties.

20. Duration of storage of personal data: Until the application or tender is assessed. The personal data of applicants who have not been selected must be deleted. The data of those who have withdrawn their application or tender must also be deleted.

21. The employer can only retain applications based on the particular express, unambiguous and voluntary consent of the person concerned, provided that their retention is necessary to achieve the purpose of the data processing in accordance with the law. This consent must be requested from the applicants after the recruitment procedure has been completed.

Data processing related to checking the use of an email account

22. If the Company provides an e-mail account to the employee - the employee can use this e-mail address and account exclusively for the purposes of their job duties, to keep in touch with each other through this account or to correspond with clients, other people and organizations on behalf of the employer.

23. The employee cannot use the e-mail account for personal purposes and cannot store personal mails in the account.

24. The employer is entitled to check the entire content and use of the e-mail account regularly - every 3 months -, in which case the legal basis for data processing is the legitimate interest of the employer. The purpose of the check is to verify compliance with the employer's provisions regarding the use of the e-mail account, as well as to verify the employee's obligations (Labour Code. §8, §52).

25. For data managing and controlling the manager or the leader with employer's authority of the Company is entitled.

26. Unless the circumstances of the inspection preclude this possibility, it must be ensured that the employee can be present during the inspection.

27. Before the audit, the employee must be informed about the employer's interest in which the audit is being carried out, who can carry out the audit on behalf of the employer - according to what rules the audit is being carried out (compliance with the principle of gradualism) and what the procedure is, - what rights and legal remedies they have in relation to the data processing associated with the audit of the e-mail account.
.
28. The principle of gradualism should be applied during the inspection, so it should be primarily determined from the address and subject of the e-mail that it is related to the employee's job duties and is not for personal purposes. The employer can examine the content of e-mails for non-personal purposes without restriction.

29. If, contrary to the provisions of these regulations, it is established that the employee has used the e-mail account for personal purposes, the employee must be asked to delete the personal data without delay. In the event of the employee's absence or lack of cooperation, the personal data can be deleted by the employer during the inspection. The employer can apply labour law consequences to the employee for using the e-mail account in violation of these regulations.

30. The employee can exercise the rights set out in the chapter on the rights of the person concerned in relation to the data processing associated with the inspection of the e-mail account.

Data management related to computer, laptop, tablet inspection

31. The computer, laptop, tablet provided by the Company to the employee for work purposes can be used by the employee exclusively for the performance of their job duties; the Company prohibits their use for private purposes; the employee cannot process or store any personal data or correspondence on these devices. The employer can check the data stored on these devices. The provisions of the previous point shall otherwise govern the inspection and legal consequences of these devices by the employer.

Data processing related to monitoring internet use at work

32. The employee can only view websites related to their job duties; the employer prohibits personal use of the internet at work.

33. The Company is the owner of internet registrations made on behalf of the Company as part of its job duties, and the Company's identifier and password must be used during the registration. If personal data is required for registration, the Company must initiate the deletion of such data upon termination of employment.

34. The employer may monitor the employee's use of the Internet at work, which and its legal consequences are governed by the provisions of this chapter.

Data processing related to monitoring the use of company mobile phones

35. The employer does not allow the use of the company mobile phone for private purposes. The employer can check the number and data of all outgoing calls, as well as the data stored on the mobile phone.

36. If the employee has used the company mobile phone for private purposes despite the ban, the check can be conducted by the employer requesting a call log from the telephone service provider and calling on the employee to make the numbers called unrecognizable on the document in the case of private calls.

Data processing related to workplace CCTV

37. The Company uses an electronic CCTV at its headquarters, premises and premises open to customers for the purpose of protecting human life, physical integrity, personal freedom, business secrets and property, which enables direct observation or recording and storage of images, sounds or images and sounds. Based on this, the behaviour of the person concerned, which is recorded by the camera, can also be considered personal data.

38. The legal basis for this data processing is the enforcement of the employer's legitimate interests and the consent of the data subject.

39. A notice or information shall be placed in a clearly visible place, clearly legible and in a manner that facilitates the information of third parties wishing to appear in the area, drawing attention to the fact that the electronic surveillance system is being used. The information shall be provided for each individual camera. This information shall include information on the fact that the electronic surveillance system is being used, as well as the purpose of making and storing the image and audio recordings containing personal data recorded by the system, the legal basis for data processing, the place of storage of the recording, the duration of storage, the person using the system (operator), the circle of persons authorized to view the data, the data security measures related to the storage of the recording, and information on the rights of the data subjects and the procedure for their enforcement.
.

40. Images and audio recordings of third parties (customers, visitors, guests) entering the monitored area may be made and processed with their consent. Consent may also be given by suggestive conduct. Suggestive conduct is especially if the natural person staying there enters the monitored area despite a sign or description informing them about the use of the CCTV installed there.

41. The recorded data can be kept for a maximum of 3 (three) working days if they are not used. Use is when the recorded image, sound, or image and sound recording, as well as other personal data, are intended to be used as evidence in court or other official proceedings

Data security measures:

a. the monitor for viewing and reviewing the images must be positioned in such a way that no other person than the authorized one can see the images while they are being broadcast
b. Surveillance and review of stored images can be carried out solely for the purpose of detecting illegal acts and initiating the necessary measures to eliminate them
c. It is not possible to record images broadcast by cameras using any device other than the central recording unit.
d. Recording media must be stored in a locked location.
e. Access to stored images can only be done in a secure manner and in such a way that the data controller can be identified
f. The review of stored images and the backup of the images must be documented
g. If the reason for the authorization ceases, access to the stored images must be terminated immediately
h. The operating system and recorded data run on a separate hard drive in the recording device. No separate backup copies of the recordings are made
i. Following the detection of an illegal act, measures must be taken to store the recording of the act and initiate the necessary official procedure immediately, and the authority must also be informed that a video recording of the act was made.
j. A person whose rights or legitimate interests are affected by the recorded image, sound, or image and sound can request - by proving their rights or legitimate interests - within three working days of the recording of the image, sound, or image and sound recording that the data controller does not destroy or delete the data.
k. A CCTV cannot be used in a room where surveillance may violate human dignity, especially in changing rooms, showers, toilets or, for example, in a medical room or its associated waiting room, nor in a room designated for employees to take breaks during work.
l. In addition to those authorized by law, the operating personnel, the employer's manager and deputy manager, and the workplace manager of the monitored area are authorized to view the data recorded by the electronic monitoring system for the purpose of detecting violations and monitoring the operation of the system.

Procedure for storing documentation containing personal data

42. The data protection officer is responsible for ensuring the secure storage of documentation containing personal data and, in the event of any impediment, to inform the managing director in writing. The medical documentation is stored at the registered office or premises of the Company.

Search and release of stored documents

43. The head of the secretariat is responsible for issuing the data stored in the archive. The list of requested documents must be sent to the employee responsible for managing the archive, who will record the issuance of documents in a register.

44. After the documents have been used, they must be returned to the head of the secretariat, who will take them back after recording them in the register.

Destruction

45. After the mandatory registration period, the data are in the medical documentation can be registered further for the purposes of medical treatment or scientific research - if justified.

46. After the mandatory registration period, if further registration is not justified, and after the withdrawal of the person's concerned consent, the documentation containing personal data must be destroyed. The documents must be destroyed using a procedure that makes their reconstruction impossible.

47. The destruction is ensured by the Company's manager and the data protection officer, considering security regulations.

V. DATA PROCESSING RELATED TO A CONTRACT

Data management of contracting partners – registration of customers and suppliers

1. The Company manages the name, birth name, date of birth, mother's name, address, tax identification number, tax number, entrepreneur's or primary producer's ID number, ID number, address, registered office, location, telephone number, e-mail address, website address, bank account number, customer number (client number, order number), online identifier (list of customers, suppliers, master purchase lists) of the natural person who has contracted with it as a customer or supplier for the purpose of concluding, fulfilling, terminating the contract, and providing a contractual discount.

2. This data processing is also considered lawful if the data processing is necessary to be taken at the request of the person concerned prior to the conclusion of the contract.

3. Recipients of personal data: employees of the Company performing customer service-related tasks, employees performing accounting and taxation tasks, and data processors.

4. Duration of storage of personal data: 8 years after the termination of the contract.

5. The natural person concerned must be informed before the commencement of data processing that the data processing is based on the legal title of the performance of the contract, the information can also be provided in the contract. The person concerned must be informed of the transfer of their personal data to the data processor.

Contact details of natural person representatives of legal entity clients, buyers, suppliers

6. The scope of personal data that can be processed: the name, address, telephone number, e-mail address, online identifier of the natural person.

7. Purpose of processing personal data: performance of the contract concluded with the Company's legal entity partner, business relations, legal basis: consent of the person concerned

8. Recipients of personal data and categories of recipients: employees of the Company performing tasks related to customer service.

9. Duration of storage of personal data: 8 years after the business relationship or the representative status of the person concerned.

10. The employee in contact with the client, buyer, or supplier must present the data collection statement to the person concerned and request their consent to the processing

of their personal data by signing the statement. The statement must be kept for the duration of the data processing.

11. The employee in contact with the client, buyer, or supplier must present the data collection statement to the person concerned and request their consent to the processing of their personal data by signing the statement. The statement must be kept for the duration of the data processing.

VI. METHOD OF STORAGE OF PERSONAL DATA, SECURITY OF DATA PROCESSING

1. The IT systems and other data storage locations of Semmelweis Premium Medical Care Services and Consulting Ltd. are located at its headquarters and at its data processors. Semmelweis Premium Services and Consulting Ltd. selects and operates IT tools used to process personal data during the provision of the service in such a way that the processed data
   a. accessible to those authorized to do so (availability)
   b. its authenticity and authentication are ensured (authentication of data processing)
   c. its immutability can be verified (data integrity)
   d. be protected against unauthorized access (data confidentiality).

2. Semmelweis Premium Services and Consulting Ltd. protects data with appropriate measures, against unauthorized access, transmission, disclosure, deletion or destruction, as well as accidental destruction, damage, and inaccessibility resulting from changes in the technology used. To protect the data files managed electronically in its various registers, Semmelweis Premium Medical Care Services and Consulting Ltd. ensures with appropriate technical solutions that the stored data - except if permitted by law - cannot be directly linked and assigned to the person concerned. In view of the current state of technology, Semmelweis Premium Medical Care Services and Consulting Ltd. ensures the protection of the security of data processing with technical, organizational and organisational measures that provide a level of protection appropriate to the risks associated with data processing.

3. Semmelweis Premium Medical Care Services and Consulting Ltd. retains the following during data processing:
   a. confidentiality: protects information so that only those who are authorized to access it can access it
      integrity: protects the accuracy and completeness of the information and the processing method
   b. availability: ensures that when the authorized user needs it, they can access the desired information and that the related tools are available.

4. The information technology system and network of Semmelweis Premium Medical Care Services and Consulting Ltd. are protected against computer-aided fraud, espionage, sabotage, vandalism, fire and flood, as well as computer viruses, computer intrusions and denial-of-service attacks. We inform users that electronic messages transmitted over the Internet, regardless of the protocol (e-mail, web, ftp, etc.), are vulnerable to network threats that lead to unfair activity, contract disputes, or the disclosure or modification of information. To protect against such threats, the data controller takes all precautions that can be expected of it. It monitors the systems to record all security deviations and provide evidence in the event of any security incident. System monitoring also allows for the verification of the effectiveness of the precautions applied.

5. Data must be recorded on a suitable quality (primarily information technology) data medium when it is generated. The person recording or recording (describing) the data is responsible for its readability and accuracy.

6. The health documentation recorded and stored at the Company - except for the images taken by diagnostic imaging procedures and the results of them - must be kept for at least 30 years from the date of recording, and the final report for at least 50 years. After the mandatory recording period, the data may continue to be recorded for the purpose of medical treatment or scientific research - if justified. If further recording is not justified, data must be destroyed. The image taken by diagnostic imaging procedures must be kept for 10 years from the date recording, and the results of them must be kept for 30 years from the date of recording.

7. The medical documentation must be managed and stored by the company's specialist and its collaborators in the information system (MedSol) used by Semmelweis University on a subsystem separate from the patients of the clinics of Semmelweis University. If the data is physically printed, it must be stored in an orderly, retrievable form, under lockable conditions. The documents must be protected from accidental destruction or intentional damage, and to prevent these events, everything must be done, considering the limitations of the possibilities, to ensure the reproducibility of destroyed or missing documents, taking into account the possibilities. The medical system must ensure the retrievability of the data.

Management of health data

8. The following persons may access the patient's personal and health data and documentation:
   a. The attending physician
   b. healthcare professionals responsible for and involved in the care
   c. healthcare professionals directly related to the treatment, outside the service provider (e.g. general practitioner, consulting doctor, doctor performing diagnostics and therapy) in the presence of the treating physician responsible for the treatment and considering the Primary Health Care Act
   d. other persons specified in Section 9(2) of the Primary Health Care Act
   e. the IT department performing the data processing, considering the Primary Health Care Act
   f. organizations and people specified in the Primary Health Care Act
   g. those specified in Annex 1, to the extent appropriate to the data processing they carry out.

Protection of the data management system environment

9. Physically printed, manually handled patient documentation (final reports, fresults, outpatient and inpatient care documentation) must be locked up at the Company's premises, offices, and archives.

10. Closed containers and regular checks of their closure must be ensured.

11. Compliance with fire safety regulations and safety measures are mandatory in places where documentation material is stored.

Measures planned to prevent damage or loss of data and to eliminate the consequences

12. The restoration of damaged or lost data and its extent - by assessing, justifying and considering the possibilities - shall be ordered in writing by the data protection officer in consultation with the managing director. If the restoration cannot be realistically implemented, the data protection officer shall prepare a written record thereof, which shall be archived in the administrative system with the filing mark "Data protection".

13. The person responsible for the omission shall be responsible for the reinstatement, if it is fair and possible. The decision on fairness and personal liability shall be within the competence of the data protection officer.

Rules for protecting against data theft

14. It is the responsibility of all employees to adhere to and promote the following principles against theft, and to properly inform the employees concerned about the legal background and this Data Protection Policy.

15. Following documentation during or related to treatment the document must be kept in a place where it can be locked and, in such cases, it must be locked.

16. In case of suspicion of theft of patient-related documentation or data, the data protection officer must be notified. In case of actual theft of data, a report must be made, and the data protection officer must be informed of the event, along with a copy of the report.
17. The data protection officer of Semmelweis University is responsible for the protection of data stored in the MedSol electronic system. Identification of the data controller, in case of entry or exit from the data management system

18. Access to the electronic data management system is only possible after the successful completion of the login procedure. During this process, the data manager - the treating physician - enters the data management system with their identifier allocated to the system and then enters the personal data of the patient they are treating, as well as the health data according to professional rules.

19. When a new data controller enters the system, the instructions generated by the system must be considered.

20. Once the service has been completed, the user exits the system, making further data access impossible.

Registration of data controllers' authorizations

21. The data management system records the rights of data controllers.

Separation of tasks of data management and maintenance and development of the data management system

22. Due to the nature of the data management system, each user can only access any data through the authorization system.

Regulation of the administration of the data management system

23. The data protection officer is responsible for keeping records of requested copies of patient documentation.

Measuring the accuracy and veracity of data

24. The employee who derives and records the data is responsible for the accuracy of the data.

25. When entering data, the provisions of professional regulations and protocols regarding the management of health documentation must be fully complied with.

Operational reliability of the data management system

26. The basis for the operational reliability of the current system is:
    a. Knowledge of the current situation and conditions
    b. Work discipline of employees performing documentation (responsible: direct supervisor)
    c. The adequacy and widespread awareness of the regulation (responsible: data protection officer)
    d. Ensuring the essential conditions (responsible: managing director);
    e. Regular and effective monitoring (responsible: data protection officer);
    f. Effective management of feedback and problems related to operations (responsible: managing director).

Technical regulation of the maintenance of the data management system

27. The space requirements for archive storage, the conditions for orderly storage, and the technical conditions for protection against fire and physical destruction must be ensured and maintained.

Regulation of the maintenance of the data management system

28. In the event of a change in legislation or a modification that becomes necessary for other reasons, the data protection and data management regulations will be modified, updated and maintained by the data protection officer.

Regulation of requirements for documenting the data management system

29. The Company's Data Management Policy also represents the basic documentation of the system.

Regulation of data protection training

30. New employees are informed about data protection by a data protection officer.

31. This Privacy Policy is available on the computer network for new employees, and they confirm their acknowledgement of its contents by logging in.

32. In case of changes, the data protection officer shall notify all affected employees within the internal IT system.

33. The provision of information on basic knowledge and its acknowledgement must be recorded in writing.

34. In the event of a change, a merged or organized information shall be used, depending on the nature and scope of the change, and the co-ordination and organization of this shall be the responsibility of the data protection officer. In the event of more significant legislative changes, comprehensive information shall be provided by a legal professional.

Data archiving procedure

35. The archiving of data stored in electronic form is ensured by the IT system storing the specific data. Paper-based patient documentation is kept by the Company.

VII. DATA AND CONTACT INFORMATION OF THE DATA CONTROLLER

1. SEMMELWEIS PREMIUM Health Care Services and Consulting Limited.
   Registered office: 1085 Budapest, Üllői út 26.
   Contacting e-mail: info@semmelweispremium.hu
   Registered: At the Metropolitan Court as a Commercial Court under the register number: 01-09-879749
   Tax number: 13916974-4-42
   Group tax number: 17784234-5-44
   Phone number: +36-1/327-0452
   Represented by: Róbert Kovács managing director

2. Data Protection Officer
   Name: Dr. Géza Freili
   Phone number: +3630/999-8165
   E-mail: freili.geza@sp.hu

VIII. RIGHTS OF DATA SUBJECTS, LEGAL REMEDIES

1. The person concerned can request information about the processing of their personal data, as well as request the correction of their personal data, or – except for mandatory data processing - its deletion or withdrawal, and can exercise their right to data portability and objection in the manner indicated when the data was collected, or at the above contact details of the data controller.

Information about the rights of the person concerned

2. The rights of the person concerned in brief:
   a. Transparent information, communication and facilitation of the exercise of the person's concerned rights
   b. Right to prior information – if personal data are collected from the person concerned
   c. Information to be provided to the person concerned and the information to be provided to them if the personal data has not been obtained by the data controller from them
   d. The person's concerned right of access.
   e. Right to rectification.
   f. The right to erasure ("the right to be forgotten")
   g. The right to restrict data processing
   h. Notification obligation related to the correction or deletion of personal data or the restriction of data processing
   i. The right to data portability
   j. The right to protest
   k. Automated decision-making in individual cases, including profiling
   l. Restrictions
   m. Informing the person concerned about the data protection incident
   n. The right to submit a complaint to a supervisory authority (right to a judicial remedy)
   o. The right to an effective judicial remedy against the supervisory authority
   p. The right to an effective judicial remedy against the controller or processor.

The rights of the person concerned in detail:

Transparent information, communication and facilitation of the exercise of rights by the affected person

3. The controller shall provide the person concerned with all information and any communication relating to the processing of personal data in a concise, transparent, intelligible and easily accessible form, in clear and plain language, in the case of any information addressed to children. The information shall be provided in writing or by any other means, including, where appropriate, by electronic means. At the request of the

person concerned, information may also be provided orally, provided that the person's concerned identity has been verified by other means.

4. The data controller must facilitate the exercise of the person' concerned rights.

5. The controller shall inform person concerned without undue delay, but in any case, within one month of receipt of the request, about the measures taken in response to the request to exercise their rights. This deadline may be extended by a further two months under the conditions laid down in the Regulation. of which the person concerned shall be informed.

6. If the controller does not take action on the person's concerned request the person concerned must be informed without delay, but at the latest within one month of reception of the request, of the reasons for not taking action and of the fact that the person concerned may submit a complaint to a supervisory authority and exercise their right for a judicial remedy.

7. The data controller provides information and information about the rights of person concerned and measures must be taken for free of charge, however, in the cases specified in the Regulation, a fee may be charged.

8. Detailed rules can be found under Article 12 of the Regulation.

<u>Right to get prior information – if personal data are collected from the person concerned</u>

9. The person concerned has the right to be informed about the facts and information related to the data processing before the data processing begins. In this context, the person concerned must be informed about:
   a. the identity and contact details of the data controller and its representative
   b. contact details of the data protection officer (if any)
   c. the purpose of the intended processing of personal data and the legal basis for the processing
   d. in the case of data processing based on legitimate interests, the legitimate interests of the data controller or a third party
   e. the recipients of the personal data – to whom the personal data are disclosed – and the categories of recipients, if any
   f. where applicable, the fact that the data controller intends to transfer the personal data to a third country or to an international organization.

10. To ensure fair and transparent data processing, data controller must inform the person concerned about the following additional information:

    a. the period for which the personal data will be stored or, if this is not possible, the criteria for determining this period

b. the right of the person concerned to request access to, rectification, erasure or restriction of processing of personal data concerning them from the controller and to object to the processing of such personal data, as well as the right of the person concerned to data portability
c. in the case of data processing based on the consent of the person concerned, the right to withdraw their consent at any time, which does not affect the lawfulness of the data processing carried out based on consent before its withdrawal
d. the right to submit a complaint to the supervisory authority
e. whether the provision of personal data is based on a legal or contractual obligation or is a prerequisite for concluding a contract, and whether the person concerned is obliged to provide the personal data, and what the possible consequences of failure to provide the data may be
f. the fact of automated decision-making, including profiling, and at least in these cases, the logic involved, and understandable information on the significance and foreseeable consequences of such processing for the data subject.

11. If the data controller intends to further process personal data for a purpose other than that for which they were collected, the person concerned must be informed about this different purpose and any relevant additional information prior to further processing.

12. The detailed rules on the right to get prior information are contained in Article 13 of the Regulation. Information to be provided to the person concerned and information to be made available to them if the personal data were not obtained by the data controller from them

13. If the data controller has not obtained the personal data from the person concerned, the person concerned must be informed by the data controller at least within a month; if the personal data are used for the purpose of communicating with the person concerned, at least upon first communication with the person concerned; or if the data are expected to be communicated to other recipients, no later than upon first communication of the personal data, at the latest when the personal data is disclosed for the first time, person concerned must be informed about the facts and information written in the previous point, as well as about the categories of personal data concerned, as well as the source of the personal data and, where applicable, whether the data originate from publicly available sources.

14. Further rules are governed by those set out in the previous point (Right to prior information).

15. The detailed rules for this information are contained in Article 14 of the Regulation.

<u>The person's concerned right of access</u>

16. The person concerned has the right to obtain information from the controller as to whether personal data concerning them are being processed and, where such processing is taking place, access to the personal data and the related information referred to in points 9 and 10 of this Chapter (Article 15 of the Regulation).

17. If personal data is transferred to a third country or to an international organisation, the person concerned has the right to be informed about the appropriate safeguards regarding the transfer in accordance with Article 46 of the Regulation.

18. The controller shall provide the person concerned with a copy of their personal data being processed. For any additional copies requested by the person concerned, the controller may charge a reasonable fee based on administration costs.

19. Detailed rules on the person's concerned right to access are contained in Article 15 of the Regulation.

The right to rectification

20. The person concerned has the right to make the Data Controller correct inaccurate personal data concerning them without undue delay, at their request.

21. Considering the purpose of data processing, the person concerned has the right to request the completion of incomplete personal data, including by means of a supplementary statement.

22. These rules are contained in Article 16 of the Regulation.

The right to erasure ("the right to be forgotten")

23. The person concerned has the right to request that the data controller erase personal data concerning them without undue delay, and the data controller is obliged to erase personal data concerning the person concerned without undue delay if:
    a. the personal data are no longer necessary for the purposes for which they have been collected or otherwise processed
    b. the person concerned withdraws their consent formed the basis of data processing and there is no other legal basis for the data processing
    c. the person concerned objects to the processing of their data and there are no overriding legitimate grounds for the processing,
    d. the personal data has been processed unlawfully
    e. the personal data must be erased for compliance with a legal obligation under European Union or Member State law to which the controller is subject
    f. the personal data is collected in connection with the provision of information society services directly to a child.

24. The right to erasure cannot be exercised if the data processing is necessary
    a. for the purpose of exercising the right to freedom of expression and information.
    b. for compliance with an obligation under European Union or Member State law to which the controller is subject to or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
    c. on grounds of public interest in the field of public health
    d. for archiving purposes in the public interest, scientific and historical research purposes or statistical purposes, where the right to erasure would likely render impossible or seriously jeopardise such processing; or
    e. to assert, exercise or defend legal claims (legitimate interest).

25. Detailed rules on the right to erasure are contained in Article 17 of the Regulation.

Right to restriction of data processing

26. In the event of restriction of processing, such personal data may be processed, with the exception of storage, only with the consent of the person concerned, 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 important public interest reasons of the European Union or of a Member State.

27. The person concerned has the right to request that the Data Controller restrict data processing if one of the following can be applied:
    a. the person concerned disputes the accuracy of the personal data, in which case restriction shall be applied for a period enabling the Data Controller to verify the accuracy of the personal data
    b. the processing is unlawful and the person concerned opposes the erasure of the data and instead requests the restriction of their use
    c. the Data Controller no longer needs the personal data for the purposes of data processing, but the person concerned requires them for the establishment, exercise or defence of legal claims; or
    d. the person concerned has objected to the processing; in this case, restriction shall be applied for a period until it is determined whether the legitimate grounds of the data controller override those of the person concerned.

28. The person concerned must be informed in advance about unblocking restriction on data processing.

29. The relevant rules are contained in Article 18 of the Regulation.

Notification obligation related to the rectification or erasure of personal data or restriction of data processing

30. The controller shall inform every recipient, to whom the personal data have been sent about all rectification, erasure or restriction of processing, unless this proves impossible or involves unreasonable effort. Upon request, the controller shall inform the person concerned about these recipients.

31. These rules are found under Article 19 of the Regulation.

The right to data portability

32. Under the conditions set out in the Regulation, the person concerned has the right to receive their personal data, which has been provided to a data controller, in a structured, commonly used and machine-readable format and has the right to transmit those data to another data controller without hindrance from the data controller to whom personal data has been provided, if:
    a. the data processing is based on consent or contract; and
    b. data processing is carried out in an automated way.

33. The person concerned may also request the direct transmission of personal data between data controllers.

34. The exercise of the right to data portability shall be without prejudice to Article 7 of the Regulation (Right to erasure ("right to be forgotten"). The right to data portability shall not be applied where the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. This right shall not adversely affect the rights and freedoms of others.

35. The detailed rules are contained in Article 20 of the Regulation.

The right to protest

36. The person concerned has the right to object, relating to their situation, at any time to processing of personal data concerning them based on public interest, the performance of a public task (Article 6 (1) e)) or legitimate interest (Article 6 (f)), including profiling based on those provisions. In such a case, the controller shall no longer process the personal data unless the controller proves compelling legitimate grounds for the processing which override the interests, rights and freedoms of the person concerned, or for the establishment, exercise or defence of legal claims.

37. Where personal data are processed for direct marketing purposes, the person concerned has the right to object at any time to processing of personal data concerning them for such purposes, including profiling where it is related to direct marketing. If the person

concerned objects to the processing of personal data for direct marketing purposes, the personal data shall no longer be processed for such purposes.

38. These rights must be expressly brought to the attention of the person concerned at latest during the first contact, and the information must be displayed clearly and separately from all other information.

39. The person concerned may also exercise the right to object by automated means based on technical specifications.

40. Where personal data are processed for scientific and historical research purposes or for statistical purposes, the person concerned shall have the right to object, on grounds relating to their situation, to processing of personal data concerning them unless the processing is necessary for the performance of a task carried out for reasons of public interest.

Automated decision-making in individual cases, including profiling

41. The person concerned has the right not to be subjected to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them.

42. This right shall not be applied if the decision:
    a. is necessary for concluding a contract between the data subject and the controller
    b. is permitted by European Union or Member State law applicable to the controller and which also lays down suitable measures to safe the rights and freedom and legitimate interests of the person concerned or
    c. is based on the explicit consent of the person concerned.

43. In the cases referred to in points a) and c) of the previous chapter, the controller is obliged to take appropriate measures to safe the rights, freedom and legitimate interests of the person concerned, including at least the right of the person concerned to obtain human intervention on the part of the controller, to express their point of view and to object to the decision.

44. Further rules are contained in Article 22 of the Regulation.

Informing the person concerned about the data protection incident

45. Where a personal data breach is likely to result in a high risk to the rights and freedom of a person, the controller shall communicate about the personal data breach to the person concerned without undue delay. That communication shall describe the nature of the personal data breach in a clear and intelligible way and shall include at least the following:

a. the name and contact details of the data protection officer or other contact person who can provide further information
b. the likely consequences of the data protection incident must be described
c. describe the measures taken or planned to be taken by the controller to remedy the data protection incident, including, where applicable, measures aimed at mitigating any adverse consequences resulting from the data protection incident.

46. The person concerned is not necessary to be informed if any of the following conditions are met:
    a. the controller has implemented appropriate technical and organisational protection measures, and these measures have been applied to the data affected by the data breach, in particular measures – such as the use of encryption – which make the data unintelligible to people who are not authorised to access the personal data
    b. the data controller has taken further measures following the data protection incident to ensure that the high risk to the rights and freedoms of the person concerned is no longer likely to materialise
    c. the provision of information would involve unreasonable effort. In such cases, the people concerned shall be informed by means of publicly published information or a similar measure shall be taken which ensures that the people concerned are informed in a similarly effective way

47. Further rules are contained in Article 34 of the Regulation.

<u>Right to restriction of data processing</u>

48. At the request of the person concerned, Semmelweis Premium Ltd. restricts data processing if one of the following conditions is met:
    a. the person concerned disputes the accuracy of the personal data, in which case restriction shall be applied for a period which allows the accuracy of the personal data to be verified; - the processing is unlawful and the person concerned opposes the erasure of the data and requests the restriction of their use instead
    b. the controller no longer needs the personal data for the purposes of the processing, but the person concerned requires them for the establishment, exercise or defence of legal claims; or - the person concerned has objected to the processing; in this case, restriction shall be applied for a period until it is determined whether the legitimate grounds of the controller override those of the data subject.

49. If data processing is subject to restrictions, personal data, except for storage, may only be processed with the consent of the person concerned, 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 important public interest reasons of the European Union or a Member State. Semmelweis Premium Ltd. shall inform the person concerned in advance about unblocking the restriction on data processing.

Right to data portability

50. The person concerned has the right to receive the personal data concerning them, which they have provided to the controller, in a structured, commonly used and machine-readable format and to transmit these data to another controller.

Right of withdrawal

51. The person concerned has the right to withdraw their consent at any time. Withdrawal of consent does not affect the lawfulness of data processing based on consent prior to withdrawal.

Right to submit a complaint to a supervisory authority (right to a judicial remedy)

52. The person concerned shall have the right to submit a complaint to a supervisory authority, especially in the Member State of their habitual residence, place of work or place of the alleged infringement, if the person concerned considers that the processing of personal data concerning them infringes the Regulation. The supervisory authority to which the complaint has been submitted shall inform the customer of the progress of the procedure and the outcome of the complaint, including the customer's right to a judicial remedy.

53. These rules are contained in Article 77 of the Regulation.

Right to an effective judicial remedy against the supervisory authority

54. Without prejudice to other administrative or non-judicial remedies, every natural and legal person has the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.

55. Without prejudice to other administrative or non-judicial remedies, every data subject has the right to an effective judicial remedy if the competent supervisory authority does not deal with the complaint or does not inform the data subject within three months about the procedural developments or the outcome of the complaint submitted.

56. Proceedings against a supervisory authority shall be brought before the courts of the Member State in which the supervisory authority is established.

57. If proceedings are brought against a decision of the supervisory authority in relation to which the Board has previously issued an opinion or taken a decision under the consistency mechanism, the supervisory authority shall be obliged to send this opinion or decision to the court.

58. These rules are contained in Article 78 of the Regulation.

Right to an effective judicial remedy against the controller or processor

59. Without prejudice to any available administrative or non-judicial remedies, including the right to submit a complaint to a supervisory authority, each person concerned shall have the right to an effective judicial remedy if, in their opinion their rights under this Regulation have been infringed as a result of the processing of their personal data not in accordance with the Regulation.

60. Proceedings against a controller or processor shall be brought before the courts of the Member State in which the controller or processor is established. Such proceedings may also be brought before the courts of the Member State in which the person concerned has their habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its official authority.

61. These rules are contained in Article 79 of the Regulation.

Rules of procedure

62. The controller shall inform the person concerned without undue delay, but in any case, within one month of the request, of the measures taken in response to the request pursuant to Articles 15 to 22 of the GDPR. If necessary, considering the complexity of the request and the number of requests, this deadline may be extended by further two months. The controller shall inform the person concerned of the extension of the deadline, indicating the reasons for the delay, within one month of the request. If the person concerned submitted the request electronically, the information shall be provided electronically, unless the person concerned requests otherwise. If the data controller does not take action in response to the person's concerned request, the controller shall inform the person concerned without undue delay, but at latest within one month of the request, of the reasons for not taking action and of the fact that the person concerned may submit a complaint to a supervisory authority and exercise their right to a judicial remedy. Semmelweis Premium Ltd. shall provide the requested information free of charge. If the person's concerned request is manifestly unfounded or, especially, excessive due to its repetitive nature, the controller may charge a reasonable fee, considering the administration costs involved in providing the requested information or taking the requested action, or may refuse to act on the request. The controller shall inform any recipient to whom or by whom the personal data have been disclosed of any rectification, erasure or restriction of processing made by it, unless this proves impossible or involves unreasonable effort. Upon request by the person concerned, the controller shall inform the person concerned of those recipients. The controller shall provide the person concerned with a copy of the personal data which are the subject of the processing. For

further copies requested by the person concerned, the controller may charge a reasonable fee based on the administration costs. If the person concerned has submitted the request electronically, the information shall be provided in electronic format, unless the person concerned requests otherwise.

Compensation and injury fee

63. Any person who has suffered material or non-material damage because of an infringement of the Data Protection Regulation shall be entitled for compensation for the damage suffered from the controller or processor. The processor shall be liable for damage caused by the processing of personal data if it has not complied with the obligations laid down in law expressly incumbent on processors or if it has disregarded or acted contrary to the lawful instructions of the controller. If several controllers or processors or both controllers and processors are involved in the same processing of personal data and are liable for damage caused by the processing of personal data, each controller or processor shall be jointly and severally liable for the entire damage. The controller or processor shall be exempt from liability if it is proved that they are not responsible for the event caused the damage.

Right to go to court

64. In the event of a violation of their rights, the person concerned may submit a complaint to the court against the data controller. The court shall proceed with the case without delay.

Data protection authority procedure

65. Complaints can be submitted to the National Data Protection and Freedom of Information Authority:

Name: Nemzeti Adatvédelmi és Információszabadság Hatóság (National Data Protection and Freedom of Information Authority)
Registered office: 1125 Budapest, Szilágyi Erzsébet fasor 22/C.
Corresponding address: 1530 Budapest, Pf.: 5.
Telephone: 061-391-1400
Fax: 061-391-1410
E-mail: ugyfelszolgalat@naih.hu
Website: http://www.naih.hu

IX. HANDLING DATA PROTECTION INCIDENTS

1. A data breach is a breach of security that results in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to, personal data transmitted, stored, or otherwise processed.

2. The prevention and management of data protection incidents and compliance with the relevant legal requirements are the responsibility of the Company's manager.

3. Access and access attempts must be logged on the IT systems, and these must be continuously analysed. If the company's employees authorized to inspect detect a data protection incident during the performance of their duties, they must immediately notify the company's manager. The company's employees are obliged to report to the company's manager or the person exercising employer rights if they detect a data protection incident or an event indicating it.

4. A data protection incident can be reported to the Company's central email address or telephone number. In the event of a data protection incident, the data protection officer – with the involvement of the IT, financial and operational managers – shall immediately examine the report, in the process of which the incident must be identified and it must be decided whether it is a real incident or a false alarm. The following must be examined and determined:
   a. the time and place of the incident,
   b. description of the incident, its circumstances and effects,
   c. the scope and quantity of data compromised during the incident,
   d. the range of people affected by the compromised data,
   e. a description of the measures taken to remedy the incident,
   f. a description of the measures taken to prevent, remedy and reduce the damage.

5. In the event of a data breach, the affected systems, people, and data must be isolated and separated, and evidence supporting the incident must be collected and preserved. Only then can the damage be repaired and lawful operations restored.

6. A record of data breaches shall be kept, which shall include the scope of the personal data concerned, the scope and number of those affected by the data breach, the date of the data breach, the circumstances and effects of the data breach, the measures taken to remedy the data breach, and other data specified in the legislation governing data processing. The data relating to data breaches included in the record shall be retained for 5 years.

In matters are not regulated in these regulations, the provisions of Hungarian and directly applicable European Union legislation shall be applied.

The data processing information of Semmelweis Premium Medical Care Services and Consulting Ltd. constitutes Annex No. 3 to these Regulations.

Budapest, 202

ANNEX No. 1
DATA PROCESSOR

DATA PROCESSOR'S NAME AND CONTACT INFORMATION	NATURE OF DATA PROCESSING ACTIVITY	SCOPE OF CONCERNED PARTIES	DATA PROCESSED	PURPOSE OF DATA PROCESSING
Hospitaly Ltd., 1143 Budapest Szobránc utca 29	Programming	Software users	name e-mail address automatically collected data (IP address, location, page, visiting data, etc.) invoice data transport data address phone number	Contract fulfilment, data storage, reports, invoicing
JacsóMédia Kereskedelmi és Szolgáltató Ltd., 2151 Fót Tarló utca 22	Website and webapps developing	Website, applications visitors, users	name e-mail address automatically collected data (IP address, location, page, visiting data, etc.) invoice data transport data address phone number, special data	Marketing activity
JacsóMédia Kereskedelmi és Szolgáltató Ltd., 2151 Fót Tarló utca 22	Website and webapps developing	Website, applications visitors, users	name e-mail address automatically collected data (IP address, location, page, visiting data, etc.) invoice data transport data address phone number, special data	Online marketing activity
JacsóMédia Kereskedelmi és Szolgáltató Ltd., 2151 Fót Tarló utca 22	CRM	Clients, newsletter recipients, partner	name e-mail address automatically collected data (IP address, location, page, visiting data, etc.) invoice data transport data address phone number	Online marketing activity
JacsóMédia Kereskedelmi és Szolgáltató Ltd., 2151 Fót Tarló utca 22	Website webapps apps support, maintenance, fixing	Website, applications visitors, users	name e-mail address automatically collected data (IP address, location, page, visiting data, etc.) invoice data	Online marketing activity

			transport data address phone number	
JacsóMédia Kereskedelmi és Szolgáltató Ltd., 2151 Fót Tarló utca 22	Programming	Software users	name e-mail address automatically collected data (IP address, location, page, visiting data, etc.) invoice data transport data address phone number	Marketing activity
JacsóMédia Kereskedelmi és Szolgáltató Ltd., 2151 Fót Tarló utca 22	Hosting	Website, applications visitors, users	name e-mail address automatically collected data (IP address, location, page, visiting data, etc.) invoice data transport data address phone number	Marketing activity
KingSol Informatikai és Tanácsadó Ltd., 1139 Budapest Forgách utca 19.	IT and E-mail system operation, software maintenance	Operating an e-mail server and software to keep internal users and external partners in touch	Name, e-mail address, special data	Ensuring communication
Blitz-Kontroll Ltd. Számviteli Szolgáltató és Tanácsadó Ltd., 8086 Felcsút szári út 23.	Accounting service	The client's employees, beneficiaries, contractual partners (suppliers, customers), and in cases prescribed by law, family members of employees	The natural person's personal identification data (including the previous name and title), gender, citizenship, tax identification number of the natural person, national health care number (TAJ number), tax number, individual entrepreneur's certificate number, primary producer identification number. Health data, personal data referring to trade union membership if it has labour law consequences under the Labor Code or tax law consequences under the Tax Act - pursuant to Article 9 (2) (b) of the Regulation.	Fulfilment of the client's tax, contribution and accounting obligations, including maintaining general ledger records, preparing summary postings, compiling reports, analysing data in reports and accounting records, and drawing conclusions to support economic decisions. Performance of labour law and payroll accounting tasks
Scope 2000 Egészségügyi, Szolgáltató és	Contribution to the provision of healthcare	The client's clients (patients)	The natural person's personal identification data (including the	The performance of services provided by the principal to its

Tanácsadó Ltd., 1094 Budapest, Páva utca 19. 5.em I/6			previous name and title), gender, citizenship, the natural person's tax identification number, national healthcare number (TAJ number), tax number, health data	clients (patients) (provision of healthcare)
Authorized doctors	Contribution to the provision of healthcare	The client's clients (patients)	The natural person's personal identification data (including the previous name and title), gender, citizenship, the natural person's tax identification number, national healthcare number (TAJ number), tax number, health data	The performance of services provided by the principal to its clients (patients) (provision of healthcare)
Frea Tanácsadó Bt., 3000 Hatvan Kertész utca 35	Marketing service, data protection officer	The client's employees, beneficiaries, contractual partners (suppliers, customers), and in cases prescribed by law, family members of employees	The natural person's personal identification data (including the previous name and title), gender, citizenship, tax identification number of the natural person, national healthcare number (TAJ number), tax number, individual entrepreneur card number, primary producer identification number	Participation in matters concerning the client that require special legal, data protection, and healthcare marketing expertise, representation before third parties and authorities in authorized matters
dr. Császár Katalin	Legal services,	The client's employees, beneficiaries, contractual partners (suppliers, customers), and in cases prescribed by law, family members of employees	Natural person identification data (including previous name and title), gender, citizenship, tax identification number of the natural person, national healthcare number (TAJ number), tax number, individual entrepreneur ID number, primary producer identification number. Health data, personal data indicating trade union membership	Participation in cases involving the client that require special legal expertise or legal assistance, representation before authorities, courts, and third parties, in accordance with the provisions of the Law on Legal Activities
Consultatio Gazdasági és Adóügyi Tanácsadó Ltd., 1121 Budapest Zugligeti út 6	Accounting service	The client's employees, beneficiaries, contractual	The natural person's personal identification data (including the previous name and	Fulfilment of the client's tax, contribution and accounting

		partners (suppliers, customers), and in cases prescribed by law, family members of employees	title), gender, citizenship, tax identification number of the natural person, national healthcare number (TAJ number), tax number, individual entrepreneur's certificate number, primary producer identification number. Health data, personal data referring to trade union membership if the Labor Code has labour law consequences or tax law consequences - based on Article 9 /2/ b) of the Regulation.	obligations, including maintaining general ledger records, preparing summary postings, compiling reports, analysing data in reports and accounting records, and drawing conclusions to support economic decisions. Performance of labour law and payroll accounting tasks

ANNEX No. 2

INFORMATION ON THE APPLICATION OF CCTV (CAMERA SURVEILLANCE SYSTEMS)

1. We inform you that Semmelweis Premium Medical Care Services and Consulting Ltd. – as data controller – uses CCTV (an electronic surveillance system) in the room indicated by the sign for the purpose of protecting human life, physical integrity, personal freedom, business secrets and property, which enables direct observation/image, sound, or image and sound recording and storage. The camera also records your behaviours.

2. Legal basis for data processing: the enforcement of the legitimate interests of the data controller.

3. Informing visitors and guests: Images and audio recordings of third parties (customers, visitors, guests) entering the monitored area may be made and processed with their consent. Consent shall be deemed to be given by suggestive conduct. Suggestive conduct is particularly the case if the natural person staying there enters the monitored area despite this information. The purpose of this data processing is set out in point 1, and its legal basis is the consent of the data subject.

4. Storage period: The recorded recordings may be kept for a maximum of 3 (three) working days if they are not used. Use is when the recorded image, sound, or image and sound recording, as well as other personal data, are intended to be used as evidence in court or other official proceedings.

5. Place of storage: registered office/location of the data controller.

6. Those entitled to view the recording: In addition to those authorized by law, the operating personnel, the employer's manager and deputy manager, and the workplace manager of the monitored area are also entitled to view the data recorded by the CCTV for the purpose of detecting violations and monitoring the operation of the system.

<u>Data security measures</u>

7. The monitor used for viewing and reviewing the images must be positioned in such a way that no other person than the authorized one can see the images while they are being broadcast.

8. Surveillance and review of stored images may be carried out solely for the purpose of detecting illegal acts and initiating the necessary measures to eliminate them.

9. It is not possible to record images broadcast by cameras using any other device than the central recording unit.

10. The recording media must be stored in a locked location. Access to stored images may only be made in a secure manner and in such a way that the data controller can be identified. The review of stored images and the backup of the images must be documented.

11. If the reason for the authorization ceases, access to the stored images must be terminated immediately.

12. The operating system and recorded recordings run on a separate hard drive in the recording device. No separate backup copies of the recordings are made.

13. Following the detection of an illegal act, measures must be taken to store the recording of the act and immediately initiate the necessary official procedure, and the authority must also be informed that a video recording of the act has been made.

Information about the rights of the person concerned and how to exercise them

14. Any person whose rights or legitimate interests are affected by the recording of image, sound, or image and sound recording data may, within three working days of the recording of the image, sound, or image and sound recording, request that the data controller not destroy or delete the data, by proving their rights or legitimate interests.

15. The rights of the person concerned are contained in detail in the Data Management Policy, which is available on the website www.semmelweispremium.hu, at the Company's headquarters and locations.

ANNEX No. 3

DATA PROCESSING NOTICE ON THE RIGHTS OF THE PERSON CONCERNED WITH REGARD TO THE PROCESSING OF THEIR PERSONAL DATA

I. INTRODUCTION

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of natural people with regard to the processing of personal data and on the free movement of such data, and repealing Regulation 95/46/EC (hereinafter referred to as the Regulation) requires that the Data Controller shall take appropriate measures to provide the person concerned with any information relating to the processing of personal data in a concise, transparent, intelligible and easily accessible form, in clear and plain language, and that the Data Controller shall facilitate the exercise of the person's concerned rights.

The obligation of prior information of the person concerned is also prescribed by Act CXII of 2011 on the right to informational self-determination and freedom of information.

We comply with this legal obligation by providing the information below.

The information must be published on the Company's website or sent to the person concerned upon request.

II. NAME OF THE DATA CONTROLLER

1. The publisher of this information, who is also the Data Controller:
   Name of the company: SEMMELWEIS Premium Health Care Services and Consulting Limited
   Registered office: 1085 Budapest, Üllői út 26.
   Company registration number: 01-09-879749
   Tax number: 13916974-4-42
   Group tax number: 17784234-5-44
   Represented by: Róbert Kovács
   Phone number:
   E-mail address: info@semmelweispremium.hu
   Website: www.semmelweispremium.hu
   (hereinafter: Company)

DESIGNATION OF DATA PROCESSORS

2. Data processor: a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the data controller; (Article 4, Article 8 of the Regulation). The use of a data processor does not require the prior consent of the person concerned, but it is necessary to inform them. Accordingly, we inform you that, in accordance with Annex 1 to the Data Protection Regulation, the data processors specified therein are authorized to act to achieve the purposes stated therein.

III. ENSURING THE LAWFULNESS OF DATA PROCESSING

Data processing based on the consent of the person concerned

1. If the Company wishes to carry out data processing based on consent, the consent of the person concerned must be requested for the processing of their personal data.

2. Consent is also deemed to be given if the person concerned ticks a relevant box when visiting the Company's website, makes relevant technical settings when using information society services, and any other statement or action that clearly indicates the person's concerned consent to the planned processing of his or her personal data in the given context. Silence, a pre-ticked box or inaction therefore does not constitute consent.

3. Consent shall be applied to all processing activities carried out for the same purpose or purposes. If the processing serves several purposes at the same time, consent shall be given for all processing purposes.

4. Where the person concerned gives their consent in the form of a written statement which also applies to other matters – e.g. the conclusion of a sales or service contract – the request for consent shall be presented in a way that is clearly distinguishable from those other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a statement containing the person's concerned consent which infringes the Regulation shall not be binding.

5. The Company may not make the conclusion or performance of a contract conditional on consent to the processing of personal data that is not necessary for the performance of the contract.

6. Withdrawal of consent should be made as easy as giving it.

7. If the personal data was collected with the consent of the person concerned, the data controller may, unless otherwise provided by law, process the collected data for the purpose of fulfilling the legal obligation applicable to it without further separate consent and even after the person's concerned consent has been withdrawn.

Data processing based on compliance with a legal obligation

8. In the case of data processing based on a legal obligation, the scope of data that can be processed, the purpose of data processing, the duration of data storage, and the recipients are governed by the provisions of the underlying legal provisions.

9. Data processing based on the legal obligation is independent of the person's concerned consent, as data processing is determined by law. In this case, the person concerned must be informed before the data processing is started that the data processing is mandatory, and the person concerned must be informed clearly and in details before the data processing is started about all the facts related to the processing of their data, especially about the purpose and legal basis of the data processing, the person authorized to process the data, the duration of the data processing, whether the data controller processes the person's concerned personal data based on a legal obligation applicable to them, and who may access the data. The information must also cover the person's concerned rights and legal remedies related to the data processing. In the case of mandatory data processing, the information may also be provided by publishing a reference to the legal provisions containing the earlier mentioned information.

Legitimate interest

10. The Company may also process the data of the person concerned based on legitimate interest.

Promoting the person concerned rights

11. The Company is obliged to ensure the exercise of the rights of the person concerned during all data processing operations.

IV. VISITOR DATA PROCESSING ON THE COMPANY'S WEBSITE (INFORMATION ON THE USE OF COOKIES)

1. The website visitor must be informed on the website about the use of cookies, and their consent must be requested - except for technically necessary session cookies.

General information about cookies

2. A cookie is a piece of data that a visited website sends to the visitor's browser (in the form of a variable name-value pair) so that it can store it and later be loaded by the same website. A cookie can be valid until the browser is closed, or for an unlimited period. Later, the browser sends this data to the server with every HTTP(S) request. This modifies the data on the user's computer.

3. The meaning of the cookie is that, by the nature of website services, it is necessary to mark a user (e.g. that they have entered the site) and be able to handle it accordingly in the following. The danger lies in the fact that the user is not always aware of this and it may be suitable for the user to be followed by the website operator or another service provider whose content is integrated into the site (e.g. Facebook, Google Analytics), thereby creating a profile about them, in which case the content of the cookie can be considered personal data.

4. Types of cookies:
   a. Technically essential session cookies: without which the site simply would not function properly, these are necessary to identify the user, e.g. to manage whether they are logged in, what they have put in the basket, etc. This is typically a session-id storage, the rest of the data is stored on the server, which is therefore more secure. There is a security aspect, if the session cookie value is not generated correctly, there is a risk of session hijacking attacks, therefore it is necessary that these values are generated correctly. Other terminologies call all cookies that are deleted when you exit the browser (one session is that a browser uses from launch to exit);
   b. User-friendly cookies: this is the name given to cookies that remember user choices, such as how the user would like to view the page. These types of cookies essentially represent the settings data stored in the cookie
   c. Performance cookies: although they have little to do with "performance", this is usually the name given to cookies that collect information about the user's behaviour during the website visit, time they spent, and their clicks. These are typically third-party applications (e.g. Google Analytics, AdWords, or Yandex.ru cookies). They are suitable for creating visitor profiles.
5. You can find information about Google Analytics cookies here:
https://developers.google.com/analytics/devguides/collection/analyticsjs/cookieusage

6. You can find information about Google AdWords cookies here:
https://support.google.com/adwords/answer/2407785?hl=hu

7. Accepting or allowing the use of cookies is not mandatory. You can reset your browser settings to refuse all cookies or to indicate when a cookie is being sent. Most browsers automatically accept cookies by default, but these can usually be changed to prevent automatic acceptance and offer you the option each time.

8. You can find information about the cookie settings of the most popular browsers at the following links:

Google Chrome: https://support.google.com/accounts/answer/61416?hl=hu
Firefox: https://support.mozilla.org/hu/kb/sutik-engedelyezese-es-tiltasa-amitweboldak-haszn
Microsoft Internet Explorer 11:

http://windows.microsoft.com/hu-hu/internetexplorer/delete-manage-cookies#ie=ie-11
Microsoft Internet Explorer 10:
http://windows.microsoft.com/hu-hu/internetexplorer/delete-manage-cookies#ie=ie-10-win-7
Microsoft Internet Explorer 9:
http://windows.microsoft.com/hu-hu/internetexplorer/delete-manage-cookies#ie=ie-9
Microsoft Internet Explorer 8:
http://windows.microsoft.com/hu-hu/internetexplorer/delete-manage-cookies#ie=ie-8
Microsoft Edge: http://windows.microsoft.com/hu-hu/windows-10/edge-privacyfaq
Safari: https://support.apple.com/hu-hu/HT201265

9. However, please note that certain website features or services may not function properly without cookies.

10. Information about the cookies used on the Company's website and the data generated during the visit:
    Data processed during the visit: Our company's website may record and process the following data about the visitor and the device used for browsing when using the website:

    a. IP address used by the visitor
    b. Type of the browser
    c. characteristics of the operating system of the device used for browsing (set language);
    d. time of the visit
    e. visited (sub)site, function or service
    f. click.

11. We retain this data for a maximum of 90 days and may use it primarily for security incident investigation.

Cookies used on the website

12. Technically essential session cookies: The purpose of data processing is to ensure the proper functioning of the website. These cookies are necessary for visitors to browse the website, to use its functions smoothly and fully, and to use the services available through the website, including, among other things, to remember the actions performed by the visitor on the specific pages or to identify the logged-in user during a visit. The duration of data processing for these cookies applies only to the visitor's current visit; this type of cookie is automatically deleted from the visitor's computer when the session ends or the browser is closed.

The legal basis for this data processing is Section 13/A. (3) of Act CVIII of 2001 on certain issues of electronic commerce services and information society services, according to which the service provider may process personal data for the purpose of providing the service that are

technically indispensable for the provision of the service. All other conditions being the same, the service provider must select and in all cases operate the means used in the provision of the information society service in such a way that personal data are processed only if this is absolutely necessary for the provision of the service and for the fulfilment of other purposes specified in this Act, but even then only to the extent and for the period necessary.

13. Cookies to facilitate use:
    These remember the user's choices, such as how the user would like to view the page. These types of cookies are essentially settings data stored in a cookie.
    The legal basis for data management is the visitor's consent.
    Purpose of data management: Increasing the efficiency of the service, enhancing user experience, and making the use of the website more convenient

14. Performance cookies:
    They collect information about the user's behaviours within the website they visit, time they spent, and their clicks. These are typically third-party applications (e.g. Google Analytics, AdWords).
    Legal basis for data processing: consent of the person concerned.
    Purpose of data processing: analysis of the website, sending advertising offers.

V. INFORMATION ABOUT THE RIGHTS OF THE PERSON CONCERNED

Information about the rights of the person concerned

1. The rights of the person concerned in brief:
    a. Transparent information, communication and facilitation to exercise the person's concerned rights
    b. Right to get prior information – if personal data are collected from the person concerned
    c. Information to be provided to the person concerned if the personal data were not obtained from them by the data controller
    d. Person's concerned rights to access
    e. The right to rectification
    f. The right to erasure ("the right to be forgotten");
    g. The right to restrict data processing
    h. Notification obligation related to the correction or deletion of personal data or the restriction of data processing
    i. The right to data portability
    j. The right to protest
    k. Automated decision-making in individual cases, including profiling
    l. Restrictions
    m. Informing the person concerned about the data protection incident
    n. Right to submit a complaint to a supervisory authority (right to a judicial remedy)

o. Right to an effective judicial remedy against the supervisory authority
p. Right to an effective judicial remedy against the controller or processor

The rights of the person concerned in detail:

Transparent information, communication and facilitation of the exercise of rights by the person concerned

2. The controller shall provide the person concerned with all information and any communication relating to the processing of personal data in a concise, transparent, intelligible and easily accessible form, in clear and plain language, especially in the case of any information addressed to children. The information shall be provided in writing or by any other means, including, where appropriate, by electronic means. At the request of the person concerned, information may also be provided orally, provided that the person's concerned identity has been verified by other means.

3. The data controller must facilitate the exercise of the person's concerned rights.

4. The controller shall inform the person concerned without undue delay, and in any case within one month of the request, of the measures taken in response to the request to exercise their rights. This deadline may be extended by further two months under the conditions set out in the Regulation. of which the person concerned shall be informed.

5. If the controller does not take action on the person's concerned request, it shall inform the person concerned without delay, but at latest within one month of the request, of the reasons for not taking action and of the fact that the person concerned may submit a complaint to a supervisory authority and exercise their right to a judicial remedy.

6. The data controller provides information and information on the rights of the person concerned and measures free of charge, however, in the cases specified in the Regulation, a fee may be charged.

7. The detailed rules can be found under Article 12 of the Regulation. Right to prior information – if personal data are collected from the person concerned

8. The person concerned has the right to be informed about the facts and information related to the data processing before the data processing begins. In this context, the person concerned must be informed:
   a. the identity and contact details of the data controller and its representative
   b. contact details of the data protection officer (if any)
   c. he purpose of the planned processing of personal data and the legal basis for the processing
   d. in the case of data processing based on the exercise of legitimate interest, the legitimate interests of the data controller or a third party

e. the recipients of the personal data – to whom the personal data is disclosed – and the categories of recipients, if any
f. where applicable, the fact that the data controller intends to transfer personal data to a third country or an international organization

9. To ensure fair and transparent data processing, the data controller must inform the person concerned of the following additional information:
   a. the period for which the personal data will be stored or, if this is not possible, the criteria for determining this period
   b. the right of the person concerned to request from the controller access to, rectification, erasure or restriction of processing of personal data concerning them, and to object to the processing of such personal data, as well as the right of the person concerned to data portability
   c. in the case of data processing based on the consent of the person concerned, the right to withdraw consent at any time, which does not affect the lawfulness of the data processing carried out based on consent before its withdrawal
   d. the right to submit a complaint to a supervisory authority
   e. whether the provision of personal data is based on a legal or contractual obligation or is a prerequisite for concluding a contract, and whether the person concerned is obliged to provide the personal data, as well as the possible consequences of failure to provide the data
   f. the fact of automated decision-making, including profiling, and at least in these cases, the logic involved, and understandable information on the significance and foreseeable consequences of such processing for the person concerned

10. If the data controller intends to further process personal data for a purpose other than that for which they were collected, it must inform the person concerned of this different purpose and any relevant additional information prior to further processing.

11. The detailed rules on the right to prior information are contained in Article 13 of the Regulation.

Information to be provided to the person concerned and information to be made available to them if the personal data were not obtained by the controller from them

12. If the data controller has not obtained the personal data from the person concerned, the person concerned must be informed by the data controller of the facts and information referred to in the previous point, as well as of the categories of personal data concerned, as well as of the source of the personal data and, where applicable, of whether the data originate from publicly available sources, no later than one month after the personal data were obtained; if the personal data are used for the purpose of communicating with the person concerned, at least upon first contact with the person concerned or if the data are

expected to be communicated to other recipients, no later than upon first communication of the personal data.

13. Further rules are governed by those set out in the previous point (Right to prior information)

14. The detailed rules for this information are contained in Article 14 of the Regulation.

The data subject's right of access

15. The person concerned has the right to obtain information from the controller as to whether or not personal data concerning them are being processed and, where such processing is taking place, access to the personal data and the related information referred to in points 8-9 of this chapter (Article 15 of the Regulation).

16. Where personal data are transferred to a third country or to an international organisation, the person concerned shall have the right to be informed of the appropriate guarantee relating to the transfer in accordance with Article 46 of the Regulation.

17. The controller shall provide the person concerned with a copy of the personal data which are the subject of the processing. For any additional copies requested by the person concerned, the controller may charge a reasonable fee based on administration costs.

18. The detailed rules on the person's concerned right of access are contained in Article 15 of the Regulation.

The right to rectification

19. The person concerned has the right to have the Data Controller correct inaccurate personal data concerning them without undue delay, at their request.

20. Considering the purpose of data processing, the person concerned has the right to request the completion of incomplete personal data, including by means of a supplementary statement.

21. These rules are contained in Article 16 of the Regulation.

The right to erasure ("the right to be forgotten")

22. The person concerned has the right to request that the data controller erase personal data concerning them without undue delay, and the data controller is obliged to erase personal data concerning the person concerned without undue delay if:

a. the personal data are no longer necessary for the purposes for which they were collected or otherwise processed
b. the person concerned withdraws their consent which forms the basis for the data processing and there is no other legal basis for the data processing
c. the person concerned objects to the processing of their data and there are no overriding legitimate grounds for the processing
d. the personal data has been processed unlawfully
e. the personal data must be erased for compliance with a legal obligation under the European Union or Member State law applicable to the controller
f. the collection of personal data took place in connection with the provision of information society services directly to children

23. The right to erasure cannot be exercised if the data processing is necessary
    a. for the purpose of exercising the right to freedom of expression and information
    b. for compliance with an obligation under the European Union or Member State law applicable to the controller or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
    c. based on public interest in the field of public health
    d. for archiving purposes in the public interest, scientific and historical research purposes or statistical purposes, where the right to erasure would likely render impossible or seriously jeopardise such processing; or
    e. to assert, enforce or defend legal claims.

24. Detailed rules on the right to erasure are contained in Article 17 of the Regulation.

<u>Right to restriction of data processing</u>

25. In the event of restriction of processing, such personal data may be processed, excepr for storage, only with the consent of the person concerned, 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 important public interest reasons of the European Union or of a Member State.

26. The person concerned has the right to request the Data Controller to restrict data processing if one of the following applies:
    a. the person concerned disputes the accuracy of the personal data, in which case restriction shall be applied for a period enabling the Data Controller to verify the accuracy of the personal data
    b. the processing is unlawful and the person concerned opposes the erasure of the data and instead requests the restriction of their use
    c. the Data Controller no longer needs the personal data for the purposes of data processing, but the person concerned requires them for the establishment, exercise or defence of legal claims or

d. the person concerned has objected to the processing; in this case, restriction shall be applied for the period until it is determined whether the legitimate grounds of the data controller override those of the person concerned.

27. The person concerned must be informed in advance of the unblocking the restriction on data processing.

28. The relevant rules are contained in Article 18 of the Regulation.

Notification obligation related to the rectification or erasure of personal data or the restriction of data processing

29. The controller shall inform any recipient to whom the personal data have been disclosed of any rectification, erasure or restriction of processing, unless this proves impossible or involves unreasonable effort. Upon request, the controller shall inform the person concerned of these recipients.

30. These rules are found under Article 19 of the Regulation.

The right to data portability

31. Under the conditions set out in the Regulation, the person concerned has the right to receive the personal data concerning them, which they have provided to a data controller, in a structured, commonly used and machine-readable format and has the right to transmit those data to another data controller without hindrance from the data controller to which the personal data has been provided, if:
    a. the data processing is based on consent or contract; and
    b. data processing is carried out in an automated way.

32. The person concerned may also request the direct transmission of personal data between data controllers.

33. The exercise of the right to data portability shall be without prejudice to Article 7 of the Regulation (Right to erasure ("right to be forgotten"). The right to data portability shall not be applied where the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. This right shall not adversely affect the rights and freedom of others.

34. Detailed rules can be found in Article 20 of the Regulation.

The right to protest

35. The person concerned shall have the right, on grounds relating to their situation, to object at any time to processing of personal data concerning them based on public interest, the performance of a public task (Article 6 (1) e)) or legitimate interest (Article 6 (f)), including profiling based on those provisions. In such a case, the controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedom of the person concerned, or for the establishment, exercise or defence of legal claims.

36. Where personal data are processed for direct marketing purposes, the person concerned shall have the right to object at any time to processing of personal data concerning them for such purposes, including profiling where it is related to direct marketing. If the person concerned objects to the processing of personal data for direct marketing purposes, the personal data shall no longer be processed for such purposes.

37. These rights must be explicitly brought to the attention of the person concerned at latest during the first contact, and the relevant information must be displayed clearly and separately from all other information.

38. The person concerned may also exercise the right to object by automated means based on technical specifications.

39. If personal data are processed for scientific and historical research purposes or for statistical purposes, the person concerned shall have the right to object, on grounds relating to their particular situation, to processing of personal data concerning them, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

<u>Automated decision-making in individual cases, including profiling</u>

40. The person concerned has the right not to be subjected to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them.

41. This right does not apply if the decision:
    a. necessary for the conclusion or performance of a contract between the person concerned and the data controller
    b. is permitted by the European Union or Member State law applicable to the controller and which also lays down suitable measures to protect the rights and freedom, and legitimate interests of the person concerned or
    c. based on the explicit consent of the person concerned.

42. In the cases referred to in points a) and c) above, the controller shall take suitable measures to protect the rights, freedom and legitimate interests of the person concerned,

including at least the right of the person's concerned to obtain human intervention on the part of the controller, to express their point of view and to object to the decision.

43. Further rules are contained in Article 22 of the Regulation.

Restrictions

44. The European Union or Member State law applicable to the controller or processor may restrict the scope of rights and obligations (Articles 12-22, 34, 5 of the Regulation) by means of legislative measures, if the restriction respects the essence of the fundamental rights and freedom.

45. The conditions for this restriction are set out in Article 23 of the Regulation.

Informing the person concerned about the data protection incident

46. Where a personal data breach is likely to result in a high risk to the rights and freedom of natural people, the controller shall communicate the personal data breach to the person concerned without undue delay. That communication shall describe the nature of the personal data breach in a clear and intelligible manner and shall include at least the following:
    a. the name and contact details of the data protection officer or other contact person who can provide further information
    b. the likely consequences of a data protection incident must be described
    c. the measures taken or planned to be taken by the data controller to remedy the data protection incident must be described, including, where applicable, measures aimed at mitigating any adverse consequences resulting from the data protection incident.

47. The person concerned is not necessary to be informed if any of the following conditions are met:
    a. the controller has implemented appropriate technical and organisational protection measures, and these measures have been applied to the data affected by the data breach, in particular measures – such as the use of encryption – that make the data unintelligible to people are not authorised to access the personal data
    b. the data controller has taken further measures following the data protection incident to ensure that the high risk to the rights and freedom of the person concerned is no longer likely to be.
    c. information would require unreasonable regulation. In such cases, the people concerned should be informed by means of publicly published information or a similar measure should be taken which ensures that the people concerned are informed in a similarly effective way

48. Further rules are contained in Article 34 of the Regulation.

Right to submit a complaint to a supervisory authority (right to a judicial remedy)

49. The person concerned shall have the right to submit a complaint to a supervisory authority, especially in the Member State of their habitual residence, place of work or place of the alleged infringement, if the person concerned considers that the processing of personal data concerning them infringes the Regulation. The supervisory authority to which the complaint has been submitted to shall inform the customer of the progress of the procedure and the outcome of the complaint, including the fact that the customer has the right to seek a judicial remedy.

50. These rules are contained in Article 77 of the Regulation.

Right to an effective judicial remedy against the supervisory authority

51. Without prejudice to other administrative or non-judicial remedies, every natural and legal person has the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.

52. Without prejudice to other administrative or non-judicial remedies, every person concerned has the right to an effective judicial remedy if the competent supervisory authority does not deal with the complaint or does not inform the person concerned within three months of the procedural developments or the outcome of the complaint submitted.

53. Proceedings against a supervisory authority shall be brought before the courts of the Member State in which the supervisory authority is established.

54. If proceedings are brought against a decision of the supervisory authority in relation to which the Board has previously issued an opinion or taken a decision under the consistency mechanism, the supervisory authority shall be obliged to send this opinion or decision to the court.

55. These rules are contained in Article 78 of the Regulation.

Right to an effective judicial remedy against the controller or processor

56. Without prejudice to any available administrative or non-judicial remedies, including the right to submit a complaint to a supervisory authority, each person concerned shall have the right to an effective judicial remedy if, in their opinion, their rights under this Regulation have been infringed as a result of the processing of their personal data not in accordance with the Regulation.

57. Proceedings against a controller or processor shall be brought before the courts of the Member State in which the controller or processor is established. Such proceedings may also be brought before the courts of the Member State in which the person concerned has their habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its official authority.

58. These rules are contained in Article 79 of the Regulation.