RMC MEDLIFE HOLDING KFT.

RMC MEDICAL ZRT.

RMC DENTART KFT.

PRIVACY POLICY

INFORMATION SHEET

Effective Date: 1 February 2020

Last modified: 1 February 2020

Version No.: V4.0

Next review due: 1 February 2021

Person in charge: Data Protection Officer

TABLE OF CONTENTS

I. GENERAL PART

1. Subject and Aim of the Policy

The aim of this policy (the "**Policy**") is to set the rules of processing, transfer, and protection of personal data. The aim of this Policy is, furthermore, to set the lawful operation of the records kept by **RMC MedLife Holding Kft.** (registered seat: 1026 Budapest, Gábor Áron utca 74-78. Building A, Floor 3; company registration number: Cg.01-09-202964) and by the following companies belonging to the company group: **RMC MEDICAL Zrt.** (registered seat: 1026 Budapest, Gábor Áron utca 74-78. Building A, Floor 3; company registration number: Cg. 01-10-048721), **RMC DENTART Kft.** (registered seat: 1026 Budapest, Gábor Áron utca 74-78. Building A, Floor 3; company registration number: Cg.01-09-276010) (hereinafter jointly referred to as "**RMC**" or "**Company Group**") in connection with the processing of personal data, to ensure the enforcement of constitutional principles of data protection and the right to informational self-determination, as well as compliance with the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, "**GDPR**") and Act CXII of 2011 on the right to informational self-determination and on the freedom of information ("**Info Act**") supplementing GDPR, also having regard to harmonization with the provisions of Act XLVII of 1997 on the processing and protection of health data and related personal data ("**Health Data Act**") and of Act XXI of 2008 on the protection of data on human genetics, on the rules of research and examinations of human genetics and of the functioning of bio-banks ("**Human Genetic Data Act**").

2. Scope of the Policy

Material scope of the Policy covers all personal data processed by RMC, as well as special categories of personal data, including genetic data.

Personal scope of the Policy covers the executive officers and employees of RMC, as well as persons employed under other legal relationship for work, temporary agency workers, workers employed by school cooperatives, and persons not being in an employment relationship, but temporarily posted under a work relationship other than employment. Personal scope of the Policy covers, furthermore, persons who receive personal data under a contract concluded with the Company Group, or process personal data on behalf of the Company Group ("**Data Processors**"). Contract for services – if it involves the processing of personal data – may only be concluded on the condition that the contracting party, including also sub-contractors, experts, advisors, and employees acting on behalf of the contracting party, makes a statement of confidentiality towards the contracting RMC entity as data controller. This statement shall be kept together with the contract for services. When processing personal data, RMC shall, furthermore, comply with the provisions of the relevant laws (in particular, GDPR, the Info Act, the Health Data Act, and the Human Genetic Data Act), and of this Policy, and shall act in accordance with their operational characteristics.

It is a precondition to entering into an employment relationship or other legal relationship for work with the Company Group that a written statement shall be made on the acknowledgement of the Policy, upon the establishment of the employment relationship. It qualifies as a material breach of employment if this statement is not sent to the RMC entity exercising employer's rights within 8 days after the establishment of employment. This statement is kept together with the personal file.

3. Data Protection Principles

The Company Group ensures compliance with data protection principles uniformly in respect of all data processing and all data subjects. When processing data, the rights and interests of data subjects shall be brought to the fore, comparing and balancing them also with the interests of the Company Group.

Collection, storage, processing, and transfer of personal data ("**data processing**") may take place only if the purpose of data processing is sufficiently specified and is lawful, there is necessary and appropriate basis for processing, and if the lawfulness of data processing is ensured during the whole process. The entities belonging to the Company Group are liable as data controllers, or in some cases as joint data controllers for the following principles to be met in respect of the processing of data:

a) It shall be ensured in connection with every processing of data that the personal data are processed in line with the principles of lawfulness, fairness, and transparency.
b) Personal data may be collected, stored, processed and transferred only for a specified, explicit purpose, and personal data may not be used for other purposes incompatible with the initial purpose; the purpose, means, and necessity of data processing shall be proportionate to each other, which shall be properly documented.
c) Processing of personal data shall be limited to what is necessary in relation to the purposes for which they are processed.
d) Personal data shall be accurate and kept up to date, every reasonable step must be taken to ensure that personal data that are inaccurate, are erased or rectified.
e) Personal data may not be stored longer than it is necessary for the purposes for which the personal data are processed; after the lapse of the processing period, personal data shall not be processed.
f) Personal data shall be processed in a way ensuring the rights of the data subjects, as well as the integrity and confidentiality of data.
g) RMC as data controller is liable for compliance with the requirements of GDPR, and also for proving such compliance. RMC shall ensure compliance with the above principles also where it acts as data processor on behalf of another data controller.
h) When setting data processing purposes, the Company Group takes into utmost consideration the special rules of medical confidentiality and the release therefrom, as well as when setting data processing guarantees, the provisions of the Health Data Act.

II. DETAILED RULES

1. Purposes for the Processing of Personal Data

RMC may process personal data only in accordance with the purpose of the initial collection of data, and for other related purposes, in accordance with the terms and conditions included in this clause.

Personal data may be collected, used, stored, or otherwise processed if it is necessary for the responsible, effective, and successful business management, in particular with regard to the following activities:

(i) taking steps necessary prior to entering into a contract or performance of a contract;
(ii) maintaining contact with contracting parties;
(iii) consideration and performance of the requests of data subjects,
(iv) establishing, exercising and defending legal claims;
(v) for statistical and scientific purposes;
(vi) implementation of business processes, organizational and asset management, performance of internal audits and inspections, financial and accounting tasks, handling management reports and evaluations;
(vii) for the purposes of safety, in particular for the safety of the assets of RMC and the data subjects;
(viii) for the performance of the legitimate interest of RMC or of a third person;
(ix) for the protection of the vital interests of the data subject; or
(x) for the performance of a legal obligation.

If special categories of personal data are processed on the basis of the consent given by the data subject, proccesing may take place after prior consultation with the Data Protection Officer.

If it is questionable whether it is lawful to process the personal data of the data subject for the above purposes, the Data Protection Officer shall be consulted before data are processed.

2. Processing of Personal Data for Other Purposes

As a main rule, RMC may use the processed personal data only for purposes for which they were initially collected (the "**Initial Purpose**").

Besides that, personal data shall be used afterwards only for related purposes listed in this Clause.

2.1 Processing of Personal Data for Secondary Purposes

Personal data may be processed for purposes other than the initial purpose (the "**Secondary Purpose**"), for the legitimate purposes of RMC only if the Initial Purpose and the Secondary Purpose are closely linked to each other, and the personal data may be used for such Secondary Purposes lawfully. When determining the Secondary Purpose, RMC shall take into consideration the context in which the personal data have been collected, in particular the following:

a) whether there is any link between the Initial and the Secondary Purpose;
b) the circumstances of the collection of the personal data concerned, in particular
c) relationship with the data subject;
d) nature of the personal data, especially sensitive data;

e) the intention of transferring the data to other data subjects;
f) existence of appropriate safeguards, which may include encryption or pseudonymization.

Before processing the personal data for Secondary Purposes, the Employee carrying out the processing of data shall consult the Data Protection Offer.

2.2 Processing of Personal Data for Other Purposes; Rules of Allowed Use

In case of every purpose different from the Initial Purpose and not covered by the concept of Secondary Purpose ("**Other Purpose**"), use of personal data for purposes other than the Initial Purpose and not covered by the concept of Secondary Purpose is lawful only if it is in line with the principle of data processing; thus, the data subject has been previously informed of the Other Purpose, and there is a legal basis appropriate for the Other Purpose.

3. Lawfulness of Processing

3.1 Legal Basis

Personal data may be processed only if and to the extent that at least one of the following legal bases is available for RMC:

a) the data subject has given consent to the processing of his/her personal data for one or more specific purposes (**consent**);

b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract (**performance of contract**);

c) processing is necessary for compliance with a legal obligation to which the controller is subject (**compliance with a legal obligation**);

d) processing is necessary for the purposes of the legitimate interests pursued by RMC or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data. Balancing test shall be performed and documented before the processing of data, and the data subject shall be informed on its core elements (**legitimate interests**);

e) processing is necessary in order to protect the vital interests of the data subject (**vital interest**).

The methodology of the balancing test is included in Clause 18 of this Policy.

3.2 Consent

Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his/her personal data. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters. Any part of such a declaration which constitutes an infringement of the law shall not be binding.

Before giving his/her consent, the data subject shall be informed of the following:

a) the purpose of data processing to which the consent is requested or to which consent shall be considered as given;

b) the right to withdraw the consent; and
c) all relevant information necessary for the data subject to be able to reach an informed decision regarding the processing of his/her personal data (e.g. nature and category of the processed personal data, third persons who may have access to the data (if any), and information on how the data subjects may exercise their rights).

Before requesting consent to the processing of personal data, the organizational unit of RMC concerned shall consult the Data Protection Officer.

The consent of children below the age of 16 years shall be lawful only if and to the extent that consent is given or authorized by the holder of parental responsibility over the child. Reasonable efforts shall be made to identify the person who holds parental responsibility over the child.

3.3 Refusal or Withdrawal of Consent

The data subject shall have the right to refuse consent or to withdraw his/her consent at any time. It shall be as easy to withdraw as to give consent. Prior to giving consent, the data subject shall be informed that withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

4. Processing of Special Categories of Personal Data

4.1 Legal Basis of Processing

Special categories of personal data may be processed only under one of the following legal titles in addition to choosing the appropriate ground set out in Clause 3 above:

a) the data subject has given explicit consent to the processing of sensitive data;
b) processing relates to personal data which are manifestly made public by the data subject;
c) processing is possible or mandatory under an act of law applicable to the controller or the data subject, thus, in particular according to the Health Data Act or the Human Genetic Data Act; it is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law;
d) processing is necessary for the establishment, exercise or defense of legal claims;
e) processing is necessary to protect the vital interests of the data subject where obtaining consent from the data subject is not possible;
f) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, or for setting up a medical diagnosis;
g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law;
h) processing is necessary for reasons of public interest in the area of public health;
i) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

4.2 Processing of Data Concerning Health and Related Personal Identification Data

4.2.1 Purpose of Processing Data

RMC may process data concerning health and personal identification data ("**Health Data**") for the following purposes:

(i) facilitating the maintenance, improvement and preservation of health;
(ii) facilitating the successful therapeutic activities of RMC, including supervisory activities;
(iii) monitoring the data subject's health status;
(iv) taking actions necessary for public health and epidemiological interests;
(v) enforcing patient rights.

In addition, Health Data may be processed, in cases defined by law, for other purposes, including in particular:

- facilitating the maintenance, improvement and preservation of health,
- facilitating the successful therapeutic activities of the patient care provider, including supervisory activities,
- monitoring the data subject's health status,
- enforcing patient rights,
- medical and epidemiological examination, analysis, planning and organizing health care, cost planning,
- statistical analysis,
- anonymization for impact assessment purposes, and scientific research,
- for the analysis of the prescription and provision of services covered by compulsory health insurance for persons entitled to health care benefits, and compliance with the rules of economic provision of medicine, medical aid and medical service, as well as financing medical care provided on the basis of a contract concluded under a separate act of law to persons entitled to benefits, and the settlement of accounts regarding price subsidy, as well as the determination, payment of social security benefits, and the repayment, reimbursement of already paid benefits,
- placement and caring for the data subject in a non-medical facility,
- assessment of working capacity,
- for the continuous and safe supply and provision of prescription medicine, medical aid and health care to persons entitled to health care benefits,
- investigation and recording of accidents at work, occupational diseases – including cases of increased exposure -, and taking the necessary occupational safety measures,
- assessment and improvement of the quality of health care services, regular review and improvement of the assessment criteria of health care services,
- for facilitating effective and safe medication to persons entitled to health care benefits, and for developing cost-effective drug therapy.

4.2.2 Persons Entitled to Process Data

The patient care provider, the head of institution, and the Data Protection Officer are entitled to process Health Data.

4.2.3 Processing of Data for the Purpose of Medical Treatment

RMC and any Processor involved shall ensure the protection of medical privacy, except if the data subject or his/her legal guardian has consented to the transfer of Health Data, or if the transfer of Health Data is compulsory under law.

If the data subject contacts RMC voluntarily, RMC considers – in the absence of a statement to the contrary - his/her consent as given to the processing of Health Data linked to therapy.

In cases defined by law, the data subject is obliged to disclose his/her personal data on the request of the patient care provider.

4.3 Processing of Genetic Data

4.3.1 Purpose of Processing

RMC processes genetic data ("**Genetic Data**") for the purpose of human genetic testing.

4.3.2 The Data Subject's Right to Information

Before taking a sample for human genetic testing, RMC, as part of a genetic consultation, educates the data subject about the purpose of taking the sample, the benefits and risks of performing or not performing the test, and the possible consequences of the test results on the data subject and his/her close relatives, on the means of storing the genetic sample and data, the possibilities of identification of data and genetic samples stored in various forms.

In addition, depending on the type of the human genetic test, RMC informs the data subject on the following:

a. in case of clinical genetic testing, on the result of the performed genetic test, its possible consequences, as well as on the genetic risks to the data subject and his/her close relatives, and on the nature of the disease;
b. in case of genetic screening, on the essence of the disease in question, the meaning of positive and negative results, as well as on the significance of the confirmatory test.

The data subject is entitled to be educated about the results of the clinical genetic testing in an individualized form, as part of a genetic consultation. Such education helps the data subject to process the possible consequences of the result in the long term, and to choose the optimal treatment options.

RMC provides genetic consultation also on the individual request of the data subject.

In case of automated data processing or encryption, RMC informs the data subject – on his/her request – on the applied IT method.

In a statement addressed to RMC the data subject may renounce his/her right to be informed on his/her genetic data, which statement may be withdrawn any time without limitation. RMC shall properly inform the data subject on this right.

4.3.3. The Right of the Data Subject to Self-Determination

Before taking the genetic testing sample – irrespective of the purpose of processing the genetic data - it is necessary to obtain the informed consent of the data subject in writing based on detailed education.

The statement of consent of the data subject shall contain the following:

a) the consent of the data subject that a genetic sample may be taken from him/her for a predefined purpose about which he/she has received detailed information;
b) the statement of the data subject that he/she consents to the use of the genetic sample or data only for the primary purpose of the sampling;
c) the statement of the data subject that he/she consents to the storage of the genetic sample or data together with personal identification data, in an encrypted or pseudonymized, or anonymized form;
d) the statement of the data subject that he/she has received and acknowledged the information referred to in Clause 4.3.2 above.

The data subject may withdraw his/her consent any time. In case of withdrawal the data subject may request the destruction of the genetic sample and all genetic data received therefrom.

After the receipt of such request, genetic samples and data may be processed only to the benefit of a close relative if the legal preconditions of processing are met.

For the purpose of preventing or getting to know the nature of his/her illness, as well as for treatment and assessment of the risk of disease to his/her offspring, the close relative is entitled to access genetic data. To this end, – if the data subject gives consent – the attending physician initiates the involvement of close relatives in the genetic consultation.

When applying the requirements of providing information and obtaining consent, RMC acts also in compliance with the rules of sections 13 and 14 of the Health Act regarding the right to information, and section 16 regarding the statement of consent.

5. Processing of Data on the Phone

RMC maintains a call center, where conversations with the call center assistant are recorded so that in case of a legal dispute RMC could retrace the events, as well as it can ensure high quality of service.

Before starting the conversation, RMC informs the data subject making the call that the call will be recorded. If the data subject does not wish the call to be recorded, he/she can object to the processing of data by interrupting the call.

6. Newsletters

RMC sends electronic messages, information, newsletters containing professional reviews and advertisements to such data subjects who have given their explicit consent thereto. Consent may be withdrawn any time by the data subject in a letter sent to the following e-mal address or on the basis of the link (info@rmc.hu) included in the newsletters.

7. Data Minimization and Quality

RMC does not process personal data that are not necessary or relevant in relation to the legitimate purposes. RMC makes reasonable efforts to ensure that personal data are accurate, complete, and up to date. RMC stores personal data for a period necessary for achieving the given purpose or for the enforcement of claims.

RMC limits personal data to what is necessary and relevant in relation to the legitimate purposes for which they are processed. RMC takes reasonable steps in order to have personal data not required for achieving the legitimate purposes safely erased.

7.1 Retention of Data

RMC stores personal data for the following periods:

a) until required by the applicable law;
b) for a period absolutely necessary for achieving the legitimate purpose for which the personal data are processed;
c) for the period necessary for meeting the applicable legal requirement;
d) in case the data are processed on the basis of consent, until the withdrawal of consent.

After the lapse of the applicable retention period RMC takes appropriate action in order to

a) erase or destroy the personal data in accordance with the relevant regulations;
b) anonymize the personal data; or
c) archive the personal data (if not prohibited by law or if it not contrary to the applicable retention plan).

RMC sets the exact retention period for the processing of personal data within the framework of each data processing activity in the records of data processing activities, and they are also included in the data processing policies.

In accordance with the provisions of the Health Data Act, RMC stores the Health Data collected from the data subject for a period of 30 years counted from their collection, and the discharge summary for 50 years. Where appropriate, Health Data processed for the purpose of treatment or scientific research may be in the records for a longer period of time.

RMC stores the image prepared by diagnostic imaging for a period of 10 years counted from its recording, and the medical report prepared from the image for a period of 30 years counted from the recording of the image.

RMC shall destroy the genetic sample and data immediately, but within 8 days the latest in case of a sample and data stored solely for human genetic research, while in case of a sample and data stored for the purpose of genetic testing after the 30th day counted from the submission of the request, within 45 days counted from the request.

RMC stores the records of the phone conversation conducted with the call center for a period of 1 year after its recording.

7.2 Data Accuracy

Personal data shall be accurate, complete, and shall be kept up to date up to the extent reasonably necessary for achieving the legitimate purpose for which the personal data is processed. It is the responsibility of RMC as controller to keep the personal data accurate, complete, and up to date. It is the responsibility of the data subject to report any changes to his/her personal data.

7.3 Processing which Does Not Require Identification

If the purposes for which RMC processes personal data do not exist any longer or do no longer require the identification of a data subject, RMC shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Policy or any applicable law.

8. Accountability and Records of Processing Activities

8.1 Obligation to Document

RMC is responsible for complying with the principles of personal data processing [GDPR Article 5, paragraph 1], and shall be able to demonstrate compliance with the principles of personal data processing. Compliance is demonstrated in particular by properly documenting decisions and the circumstances substantiating the decisions related to processing, information and statements addressed to the data subjects, and the statements given by the data subjects.

Data processing policies shall be reviewed by the Data Protection Officer regularly, at least once a year.

If personal data are processed after performing a balancing test, on the basis of legitimate interest, RMC records and stores in writing, in a documentable and retrievable format, the findings and results of the balancing test and all related documentation. A balancing test template is included in Annex No. 3, and the detailed rules of performing the balancing test are set out in Chapter 18 hereof.

If personal data are processed after carrying out an impact assessment, RMC records and stores in writing, in a documentable and retrievable format, the findings and results of the impact assessment and all related documentation. A template for impact assessment is included in Annex No. 4, and the detailed rules of carrying out the impact assessment are set out in Chapter V hereof.

8.1.1 Documentation and Storage of Consents

If out of the legal bases for processing of personal data (GDPR, Article 6), the personal data in question are processed on the basis of the consent given by the data subject, RMC shall be able to demonstrate that the data subject has given consent to the processing of his/her personal data. If any doubt is raised during the processing of personal data regarding the request of the data subject's consent, necessary guidance shall be sought from the Data Protection Officer. All statements of the data subjects – made in writing, online, in an e-mail or otherwise - containing consent to the data processing activities of RMC shall be recorded, filed, and stored in a documentable and retrievable format. Statements of consent shall be recorded in accordance with the records management rules in cases where the data subject has consented to the processing of his/her personal data. A sample statement of consent is included in Annex No. 5. All fields of specialization involved shall carry out the tasks connected to the statements of consent (recording, filing, storage, etc.) in the course of carrying out their own tasks, at their own discretion, in consultation with the Data Protection Officer.

Withdrawal of the data subject's consent shall be ensured, documented, and the statement of withdrawal shall be stored in the same way as giving consent.

If the legal basis of processing is the consent of the data subject, then in case of withdrawal of the consent, RMC erases the data processed on the basis of the consent in accordance with Article 17 of the GDPR.

RMC retains the statements of consent and the statements on the withdrawal of consent for a period specified in the relevant data processing policy.

8.1.2 Informing Data Subjects and Documentation thereof

RMC shall take appropriate measures in order to provide all necessary information regarding the processing of personal data and all other information to the data subjects in a concise, transparent, intelligible and easily accessible form, using clear and plain language, especially in case of any information addressed to children.

It shall be recorded in a documentable and retrievable format by the organizational unit providing information that the information has been addressed to the data subject and that the data subject has received the information.

8.2 Records of Processing Activities

In the course of processing personal data RMC shall ensure compliance with data protection laws, in particular with Article 30 of the GDPR under which it maintains a record of data processing activities. RMC maintains the record of data processing activities in an electronic format. The record contains the following information:

a) contact details of RMC;
b) the purposes of data processing;
c) a description of the categories of data subjects and of the categories of personal data;
d) the categories of recipients to whom the personal data have been or will be disclosed including recipients' geographical location;
e) if personal data are transferred to a non-EEA country not ensuring an adequate level of protection, or data are transferred on the basis of an adequacy decision, then the country ensuring a not adequate level of protection or in case of data transfer on the basis of an adequacy decision the target country, and in case of data transfer to a country not ensuring adequate level of protection, the suitable safeguards;
f) where possible, the envisaged time limits for erasure of the different categories of data;
g) where possible, a general description of the technical and organizational measures;
h) where RMC acts as processor, the name and contact details of the controller, and the categories of data processing activities carried out on behalf of the controller; and
i) if applicable, the fact of joint processing, and the definition of the involved controller.

9. Data Protection Framework – Responsibilities

RMC pays special attention to the protection of personal data; thus, it takes all necessary measures for the protection of personal data of natural persons involved, and for ensuring the rights connected to the protection of personal data.

9.1 Management

The management of RMC adopts strategic decisions concerning data protection. Before adopting decisions concerning data protection, the management consults the Data Protection Officer.

9.2 Data Protection Officer

By RMC, a Data Protection Officer as defined in Article 38 of the GDPR is in charge.

The Data Protection Officer (DPO) is in charge of the cases falling under the scope of the Policy. The Data Protection Officer is independent in his/her activities under the Policy, he/she cannot be given orders in connection with his/her tasks.

The tasks of the Data Protection Officer are, in particular:

a) to arrange for the proper handling of personal data breaches in accordance with the provisions of Clause II.12;
b) to cooperate and provide assistance in the course of the adoption of decisions concerning data protection;
c) to facilitate and ensure the exercise of the rights of the data subjects;
d) to take steps to investigate notifications and complaints received;
e) to maintain the records of processing activities and to keep them up to date;
f) to monitor compliance with the Policy;
g) to comment on or to have an expert with appropriate expertise comment on the drafts of internal regulatory documents received concerning data protection matters;
h) to monitor compliance with the provisions of data protection laws, the Policy and other regulations concerning data protection, and with data protection requirements;

i) to monitor privacy compliance in respect of the practices, regulations, commercial contracts applied by RMC, including also the data processing agreements;
j) to cooperate with and to act as a contact point for the supervisory authority; and
k) to continuously monitor and assess the privacy risks of RMC.

The Data Protection Officer shall be involved in every matter concerning data protection. The management of RMC ensures all necessary funds for carrying out the tasks of the Data Protection Officer.

9.3 Employee Obligations

Employees:

a) may have access to the personal data processed by RMC solely in performance of their duties, and to the extent necessary for achieving the legitimate purpose;
b) shall report all breaches and events concerning personal data to their direct supervisor or to the Data Protection Officer; and
c) shall inform RMC within reasonable time on any changes to their personal data. RMC shall not be responsible for any damage resulting from the failure of the employee to comply with this obligation, if RMC has timely and properly informed the employee thereon.

10. Requirements of Information Given to Data Subjects

RMC ensures that the data subjects are properly informed on the purpose of processing personal data, as well as, on request to this effect, RMC provides any other information regarding personal data processing related to the data subjects.

RMC shall provide the information on the details of the processing of their personal data, as required by Articles 13 and 14 of the GDPR, in the form of appropriate privacy policies. Information shall be provided to the data subjects in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

Before the start of a new data processing activity, the organizational unit responsible for the envisaged processing activity shall contact the Data Protection Officer to take steps for the preparation of the relevant privacy policy.

When complying with the requirements set out in this clause regarding the information to be provided to data subjects, RMC also takes into account the proper application of the provisions of sections 13 and 14 of the Health Act regarding provision of information.

10.1 Information to be Provided where Personal Data are Collected from the Data Subject

RMC shall inform the data subject on the following:

a) the primary and secondary purposes for processing of personal data, and the related legitimate interest of RMC, if any;
b) the identity and the contact details of the controller;
c) the nature and categories of the processed personal data;
d) the categories of third persons to whom personal data are transferred (if any);
e) information on how to assert the rights of data subjects, including information on the right to lodge a complaint with NAIH;
f) if RMC intends to transfer personal data to a country not ensuring adequate level of protection, or on the basis of an adequacy decision, the suitable safeguards, as well as the means by which to obtain a copy of such safeguards or where they have been made available;

g) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
h) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, and of the possible consequences of failure to provide such data; and
i) the existence of automated decision-making, including profiling, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

10.2 Information to be Provided where Personal Data are Not Collected from the Data Subject

If the personal data have not been collected directly from the data subject, RMC shall inform the data subject on the following:

a) information listed in Clause II.10.1;
b) the (publicly accessible) sources of the personal data;
c) such information shall be provided
    i. at the time of recording the personal data in a database of RMC, but within one month after obtaining the personal data, the latest; or
    ii. if the personal data are disclosed to other recipients, at the latest when the personal data are first disclosed to another recipients.

10.3 Exceptions

Provisions of Clause II.8.2 do not apply if

a) the provision of such information to the data subjects proves impossible or would involve a disproportionate effort; or
b) it would lead to disproportionately high costs; or
c) obtaining or disclosure is expressly laid down by law to which RMC is subject and which provides appropriate measures to protect the data subject's legitimate interests.

11. Rights of the Data Subjects

Data subjects whose personal data are processed by RMC as controller, shall be entitled to the following rights under this Policy.

11.1 Right of Access

All data subjects are entitled to receive confirmation on the processing of his/her data processed by or on behalf of RMC. In case the data subject’s data are processed, the confirmation shall include the following, if possible:

a) the legitimate purposes of the processing;
b) the categories of personal data concerned;
c) the categories of the recipients of the personal data concerned;
d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
e) the source of the personal data, where the personal data are not collected from the data subject;
f) the existence of automated decision-making, including profiling, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject; and
g) in case of data transfer to a country not ensuring adequate level of protection, or on the basis of an adequacy decision, the appropriate safeguards.

In addition to the confirmation, – on the request of the data subject - RMC provides the data subject with the following information:

a) information on the right of the data subject to request any time the rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
b) the right to lodge a complaint with NAIH;
c) the possibility of judicial redress; and
d) if relevant, the possibility of claiming damages in case of a breach of binding corporate rules.

11.2 Right to Rectification

The data subject shall have the right to request the rectification of inaccurate personal data concerning him/her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

11.3 Right to Erasure

The data subject shall have the right to request the erasure of personal data concerning him/her if

a) his/her personal data are no longer necessary in relation to the legitimate purposes for which they were collected or otherwise processed;
b) the data subject withdraws consent, and there is no other legal ground for the processing;
c) the data subject successfully objects to the processing pursuant to Clause II.11.7 hereof;
d) the data subject's personal data have been unlawfully processed; or
e) the personal data must be erased for compliance with a legal obligation.

11.4 Right to Restriction of Processing

The data subject shall have the right to request the restriction of processing of personal data concerning him/her if

a) the accuracy of the personal data is contested by the data subject, for a period necessary for RMC to verify the accuracy of the personal data in question;
b) the processing is unlawful;
c) RMC no longer needs the personal data for any legitimate purpose, but they are required by the data subject for the establishment, exercise or defense of legal claims; or
d) the data subject has objected to processing pursuant to Clause II.11.7 hereof, pending the verification of the legitimate interests of RMC.

Restriction of the processing of the data subject's personal data may affect the services provided by RMC.

During the period of restriction, personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defense of legal claims or for the protection of the rights of another natural or legal person.

RMC shall inform the data subject before the restriction of processing is lifted.

11.5 Obligation to Notify

RMC notifies all recipients to whom the personal data have been disclosed on any rectification or erasure of personal data or restriction of processing carried out in accordance with under Clauses II.11.2-II.11.4 above, unless this proves impossible or involves disproportionate effort. On request, RMC informs the data subject on such recipients.

11.6 Right to Data Portability

The data subject shall have the right to receive the personal data concerning him/her that he/she has provided to RMC, in a structured, commonly used and machine-readable format if

a) the processing is based on consent of the data subject; or
b) the processing is based on the performance of a contract concluded with the data subject, and it is carried out by automated means.

11.7 Right to Object

The data subject shall have the right to object, on grounds relating to his/her particular situation, at any time to the processing of his/her personal data which is done in the course of the performance of a task carried out in the public interest or in the exercise of official authority, or which is necessary for the purposes of enforcing the legitimate interests of RMC or of a third party.

The data subject shall have the right to object, furthermore, to the processing of his/her personal data, which is based on legitimate interest, unless RMC demonstrates compelling legitimate grounds for the processing which provide legitimate interest for RMC to process the data, or are related to the establishment, exercise or defense of its legal claims.

11.8 Provisions regarding the Procedure for Exercising the Rights of the Data Subjects

The data subject shall send his/her request to the contact person or point named in the relevant privacy policy. If the data subject is an Employee of RMC, he/she may exercise his/her rights using the form included in Annex No. 6.

Before examining its obligation to fulfill the request, RMC may request the data subject to do the following:

a) to name the type of personal data to which he/she requires access;
b) to name the circumstances under which RMC has collected the data;
c) to credibly verify his/her identity; and
d) in case of a request for rectification, erasure, restriction, or objection, to name the reasons why the personal data are inaccurate, incomplete, or are not processed according to the applicable laws or this Policy.

Within one month after the receipt of the request, the Data Protection Officer or the employee responsible for maintaining contact with the natural person in question shall inform the data subject in writing

a) on the opinion of RMC regarding the submitted request, and measures taken or envisaged pursuant to the request;
b) if further information or clarification is required for the effective fulfillment of the request; or

c) on the reasons of delay and the latest deadline by which RMC will inform the data subject on its opinion, which shall not be later than two months after the receipt of the request.

The person receiving the request shall inform the Data Protection Officer on the content of the request within 3 days after its receipt.

If RMC fails to take any action pursuant to the request of the data subject, it shall inform the data subject without delay, but within one month after the receipt of the request the latest, on the following:

a) the reasons for not taking any action;
b) the possibility of lodging a complaint with NAIH, and
c) of seeking judicial remedy.

11.9 Right to Claim Damages

The data subjects shall have to right to claim damages from RMC for the compensation of the pecuniary and non-pecuniary damage (payment of restitution) they have suffered because of the breach of this Policy.

The data subject may bring an action for damages before the local or regional court having jurisdiction according to the registered seat of RMC. The data subject may submit his/her claim for damages also to the competent court having jurisdiction according to the place of habitual residence of the data subject.

11.10 Complaint

The data subject may lodge a complaint in accordance with the provisions of Clause II.12 if

a) the response of RMC to the request is not acceptable for the data subject (e.g. refusal to fulfill the request);
b) the data subject has not received a response as set forth in Clause II.11.8; or
c) the deadline set for the data subject under Clause II.11.8 proved to be unreasonably long for the data subject considering the circumstances, and the data subject has not received feedback, despite the objection submitted, to a request for a response within a reasonably shorter period of time in consideration of the circumstances.

11.11 Rejection of the Request

RMC may reject the fulfillment of the request submitted by the data subject if

a) the request is not accurate enough to be fulfilled;
b) the identity of the data subject cannot be ascertained with reasonable efforts; or
c) it is submitted by the data subject repeatedly within an unreasonably short period of time, or if the request has been submitted clearly in bad faith. A request submitted repeatedly within three (3) months qualifies as a request submitted within an unreasonably short period of time.
d) in case of mandatory processing of personal data required by law, the data subject submits a request against the processing of data for objection, restriction or for erasure of data.

12. Complaint Handling Process

Every data subject is entitled to lodge a complaint, without prejudice to their rights and possibilities for judicial redress, if he/she thinks that his/her rights under privacy laws or this Policy have been violated. The employee taking in the complaint shall forward it without delay to the Data Protection Officer.

Employees may lodge their complaints regarding the processing of their personal data directly with the Data Protection Officer.

The Data Protection Officer shall:

a) arrange for the immediate investigation of the complaint, and inform the complainant on the results of the investigation within one month after the receipt of the complaint;
b) take the actions necessary for dealing with the complaint, in particular prepare a response to the complaint to the data subject, and if necessary in order to deal with the complaint, contact the organizational unit involved in order to take the necessary actions for dealing with the complaint; and
c) monitor the implementation of actions taken in the course of dealing with the complaint.

The Data Protection Officer shall have the right to contact any competent authority in the matter affected by the complaint, and to negotiate the actions to be taken in the matter.

Within one month after the receipt of the complaint, the Data Protection Officer shall inform the data subject in writing

a) on the opinion of RMC regarding the complaint, and actions taken or envisaged pursuant to the complaint; or
b) in case of a delay, on the reasons thereof, and the latest deadline by which RMC will inform the data subject on its opinion, which shall not be later than two months after the receipt of the request.

13. Requirements of Security and Confidentiality

RMC takes appropriate measures for protection against unauthorized access and other unlawful processing of personal data, e.g. for the event of accidental loss or destruction, damage, alteration, or disclosure.

13.1 Data Security

RMC implements commercially reasonable and appropriate technical, physical and organizational measures for protection against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data.

13.2 Data Protection by Design and by Default

RMC implements appropriate technical and organizational measures for the effective implementation of data protection principles and for the realization of appropriate safeguards integrated into the processing, taking into account the art and cost of implementation and the nature, scope, context and purposes of processing, as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing.

RMC implements appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed.

13.3 Access Management

Employees may have access to personal data processed by RMC only in performance of their duties, and to the extent necessary for achieving the legitimate purpose. Employees entitled to access personal data shall be bound by the obligation of confidentiality.

14. Personal Data Breach

14.1 General Rules regarding Personal Data Breach

In the case of a personal data breach, the Data Protection Officer shall without undue delay, but not later than within 72 hours after having become aware thereof, notify the personal data breach to the competent supervisory authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

The notification shall, at least

a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data concerned;
b) communicate the name and contact details of the contact point where more information can be obtained;
c) describe the likely consequences of the personal data breach;
d) describe the measures taken or proposed to be taken to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

RMC documents any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken.

When the personal data breach is likely to result in high risk to the rights and freedoms of natural persons, RMC notifies the data subject without undue delay, using clear and plain language, on the nature of the personal data breach and on the information listed in points (b), (c), and (d) above.

The notification of the data subject referred to above is not required if any of the following conditions are met:

a) appropriate technical and organizational protection measures have been implemented, and such measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorized to access it, such as encryption;
b) subsequent measures have been taken which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialize; or
c) notification would involve a disproportionate effort.

In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

14.2 Procedure to be Followed in case of a Personal Data Breach

All employees of RMC, as well as persons employed by RMC on the basis of a legal relationship other than employment, and all other persons to whom this Policy applies, are obliged to report without undue delay all personal data breaches they become aware of to

the Data Protection Officer, and shall cooperate in the course of the investigation, termination, and the mitigation of the consequences of the personal data breach.

The person becoming aware of a personal data breach shall report such breach to the Data Protection Officer for action without undue delay.

The Data Protection Officer shall take the necessary action for the investigation, termination, and mitigation of the consequences of the breach, as well as for monitoring the implementation of such actions.

15. Data Protection Impact Assessment

Prior to the processing of data RMC shall carry out an impact assessment ("**DPIA**") of the impact of the envisaged processing operations on the protection of personal data, if the processing

a) is highly likely to result in (high) risk to the rights and freedoms of the data subjects; and/or
b) it covers also the processing of special categories of personal data referred to in Clauses 4 and III3; and/or
c) involves systematic monitoring of a publicly accessible area.

The head of the organizational unit affected by the new processing of data shall be responsible, in respect of the processing of data carried out by the organizational unit question, to carry out the DPIA and to consult the Data Protection Officer in connection therewith. If necessary, but at least upon changes to the risk of data processing activities, RMC reviews and evaluates compliance of the data processing activities with the DPIA.

Should the data protection impact assessment establish that in the lack of measures adopted by RMC for the mitigation of risks the processing will presumably entail a high risk, RMC shall consult the supervisory authority prior to the processing of data.

16. Transfer of Personal Data

16.1 Enquiries from Authorities

Any request for the transfer of personal data may be fulfilled only with the approval of the Data Protection Officer or the management. In case of enquiries from authorities or courts the Legal Department, while in case of enquiries from NAIH the Data Protection Officer is entitled to transfer data, solely in writing, and only if

a) the enquiry has been received in writing from an authority entitled to request data, duly signed, and an original copy of such request is available to RMC, and
b) in its enquiry the body requesting data has named the person of whom the abovementioned body or authority requests the personal data, as well as the type of data requested and the purpose of the request, except if the competent authority is carrying out an on-site inspection.

Exceptionally (in particularly justified cases) the Legal Department may fulfill requests of courts and authorities if the original copy of the request is not available (because, for example, the request was received via fax due to the urgent nature of the investigation). However, also in such cases it is a precondition to fulfilling the request that it meet the other conditions set forth above.

16.2 Transfers of Data Abroad

In case of certain processing activities RMC may transfer personal data to third countries outside the European Economic Area or to international organizations ("**Transfers of Data Abroad**").

Transfers of Data Abroad may take place where the Commission of the European Union (the "**Commission**") has decided that the third country ensures an adequate level of protection for personal data ("**Adequacy Decision**")[1].

In the absence of an Adequacy Decision RMC may transfer personal data only if the recipient controller or processor has provided appropriate safeguards in relation to the processing. Such appropriate safeguards may be, without requiring any specific authorization from the competent supervisory authority, for example:

a) standard data protection clauses adopted by the Commission or standard data protection clauses adopted by a supervisory authority and approved by the Commission;
b) an approved code of conduct together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights;
c) an approved certification mechanism together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

In the absence of appropriate safeguards transfers of data may take place only on one of the following conditions:

a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
d) the transfer is necessary for important reasons of public interest;
e) the transfer is necessary for the establishment, exercise or defense of legal claims;
f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;
g) the transfer is made from a register which, according to Union or Member State law, is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case.

Where a transfer could not be based on adequacy, there are no appropriate safeguards available, and none of the derogations for a specific situation is applicable, a transfer to a third country may take place only if

a) the transfer is not repetitive,
b) concerns only a limited number of data subjects,

[1] Andorra, Argentina, Faroe Islands, Guernsey, Israel, Jersey, Canada, Isle of Man, Switzerland, Uruguay, USA, New Zealand.

c) is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and
d) the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data.

In such cases RMC shall inform the NAIH of the transfer. The controller shall, in addition to complying with its general obligation to provide information, inform the data subject of the transfer and on the compelling legitimate interests pursued.

17. Processors

Data processing required in the course of the activities of RMC is sometimes carried out by other persons ("**Processors**") on the basis of a permanent or ad hoc assignment given by RMC. Processors may be permanently engaged for example for performing administrative tasks in connection with the services connected to the activities of RMC, and for the maintenance of the IT system. To the engagement of Processors, laws on data privacy, in particular the provisions of GDPR and the Info Act shall be applicable.

Only persons and organizations may be engaged as processors who provide sufficient guarantees to implement appropriate technical and organizational measures ensuring the lawfulness of processing and the protection of the rights of the data subject.

In the contract to be concluded with RMC the Processors shall explicitly agree to process the data in compliance with the requirements of the GDPR. In accordance with Article 28 of the GDPR, the contract between RMC and the Processors shall include at least the following:

a) statement of the Processor that it has implemented appropriate technical and organizational measures in compliance with the GDPR and ensuring the protection of the rights of the data subject;
b) the Processor shall not engage another processor (sub-processor) without prior specific or general written authorization of RMC;
c) subject-matter and duration. as well as the nature and purpose of the processing carried out by the Processor, the type of personal data and categories of data subjects;
d) consent of the Processor that it processes the personal data only according to written instructions from RMC, including with regard to transfers of personal data to a third country or an international organization, unless processing is required by Union or Member State law to which the person carrying out the outsourced activities is subject;
e) the Processor shall assist RMC in responding to requests for the exercise of rights of the data subjects;
f) the Processor undertakes in a separate clause to ensure that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

The Processors shall maintain a record in accordance with Article 30 of the GDPR of processing activities carried out on behalf of RMC, as well as they shall immediately notify RMC of beaches of rules regarding processing of personal data they might become aware of.

The Processors shall provide RMC with all information necessary to certify compliance with the obligations under the GDPR.

18. Joint Controllers

RMC sometimes determines the purposes and means of processing arising from its activities jointly with two or more controllers; such cases qualify as joint processing of data. The joint controllers shall determine in a transparent manner their respective responsibilities for compliance with the obligations under the GDPR, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14 of the GDPR, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by law to which the controllers are subject. The arrangement shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects. The essence of the arrangement shall be made available to the data subjects.

19. Priority Interest

RMC may ignore its obligations under this Policy or the rights of the data subjects solely under the conditions and to the extent set forth in this Clause and in accordance with the provisions of law.

The obligations of RMC under this Policy or the rights of the data subjects may be ignored taking into account the context of the case, in case of an urgent need up against the legitimate interests of the data subject (the "**Priority interest**"). There is an urgent need qualifying as Priority Interest if

a) the legitimate economic interests of RMC require protection, in particular:
    (i) health or safety of employees or clients;
    (ii) intellectual property rights, business secrets, or goodwill of RMC;
    (iii) smooth operation of RMC;
    (iv) the confidentiality of an envisaged sale and purchase, acquisition; or
    (v) involvement of financial, business, tax or other advisors;
b) prevention or investigation of an unlawful or presumably unlawful action (including cooperation with law enforcement);
c) establishment, exercise or defense of legal claims;
d) for the protection of the rights and interests of RMC, its employees or other persons.

19.1 Exceptions Applicable in case of a Priority Interest

In case a Priority Interest exists, one or more of RMC's following obligations and the following rights of the data subject may be ignored:

a) Clause II.1 (purposes of processing);
b) Clauses II.10.1 and II.10.2 (providing information on data collected from the data subject and not from the data subject); and
c) Clause II.9 (rights of the data subject).

19.2 Processing of Special Categories of Data in case of a Priority Interest

The application of the requirements set forth in Clauses II.4 and III.3 regarding special categories of personal data may be ignored only because of Priority Interests defined in points (a) (i), (ii) and (v), b)-d) of Clause II.17.

19.3 Prior Consultation

The Data Protection Officer shall be consulted prior to ignoring the obligations of RMC or the rights of the data subject because of a Priority Interest.

20. Balancing Test

In all cases where processing is intended to be based on the legitimate interest of RMC or of third parties, a balancing test shall be carried out prior to the processing. The purpose of the balancing test is to establish whether the legitimate interest of the controller or of third parties takes precedence over such interests or fundamental rights and freedoms of the data subject that require the protection of his/her personal data. Special care shall be exercised in all cases where the data subject is a child.

Balancing tests shall always be carried out in a transparent manner, and it shall be documented using plain language, in a form accessible for everyone. According to point b) of Article 14 paragraph (2) of the GDPR, the data subject shall be informed of the legitimate interest and the context of its enforcement. The data subject has the right to object to data processing based on legitimate interest; his/her attention shall be explicitly drawn to this right when providing information on such processing. The Data Protection Officer is responsible for initiating procedures connected to objections and enquiries against the processing of data on the basis of legitimate interest.

The balancing test shall include the following mandatory elements:

a) the purpose of processing;
b) methodical and systematic description of processing;
c) description of how the data subjects' rights are ensured;
d) description of how the principles of processing are ensured;
e) technical and organizational measures introduced for the protection of personal data;
f) assessment of the effect of data processing on the freedoms and fundamental rights of the data subject; and
g) the result of the balancing test.

The template necessary for performing the balancing test is included in Annex No. 3 hereof.

21. Data Protection Awareness and Training

RMC organizes training at least once a year to the Employees having access to personal data on the contents of the Policy and their obligation of confidentiality. Continuous, professional education, specialized on certain data processing operations, shall be provided to persons performing important tasks in connection with the processing of personal data.

22. Monitoring Compliance

22.1 Checks

The Data Protection Officer carries out checks on the compliance of processes involving the processing of personal data with the provisions of privacy laws and the Policy. RMC may also resort to the assistance of an external advisor when checking privacy compliance.

22.2 Mitigation of Violations

RMC shall arrange for taking the appropriate measures in order to eliminate circumstances revealed by the checks, causing the violation of the Policy.

22.3 Consequences of Policy Violation

Violation of this Policy by an Employee qualifies as, from the point of view of the employment, a serious breach of obligations of the Employee, which may serve as a basis for applying adverse legal consequences against the Employee or the termination of his/her employment with immediate effect. If this Policy is violated by personnel not qualifying as

Employee, it may serve as a basis for RMC to terminate the contract concluded with such person.

III. PROCESSING OF EMPLOYEE DATA

1. Purpose of Processing Employee Data

As employer, RMC processes the personal data of Employees solely in accordance with the following initial purposes of data collection. Processing of Employee personal data for other purposes (e.g. administration in connection with participation in free time activities) is possible only if there is an appropriate legal basis, after information has been provided under the terms of Clause II.7. and, if necessary, the consent of the Employee has been obtained.

The Employer collects, uses, stores, or otherwise processes the personal data of Employees for the following purposes:

a) **Human resources and organizational management**: processing necessary for the performance of the contract of employment or other contract with the Employee (or in order to take steps at the request of the Employee prior to entering into a contract), or for the administration of recruitment, selection, and posting, allowances, payments, tax administration, career and talent management, performance evaluation, training, travel and reimbursement of expenses, employee communication, international assignments, dispute resolution and litigation, community events organized by the company; or
b) **Execution of electronic business processes and internal management**: work organization, working time records, RMC asset management, internal audits and investigations, implementation of business controls, ensuring effective electronic communication; or
c) **Health and safety**: activities related to occupational health and safety, protection of assets and goodwill of RMC, protection of Employees, access management, and checks of compliance with RMC policies; or
d) **Organizational analysis and management reports**: conducting Employee surveys, processing necessary for management reports and analyses; or
e) **Compliance with the provisions of law**: compliance with laws applicable to RMC and with sector-specific rules; or
f) **Protection of vital interests of the Employees**: processing is necessary for the protection of the vital interests of the Employees, e.g. urgent health reasons.

2. Legal Basis for Processing Employee Data

RMC processes personal data of Employees in the following cases:

a) on the basis of consent given by the Employee (in case the appropriate conditions are met);
b) if processing is necessary for the conclusion of the contract of employment and for the performance of the employment relationship;
c) if processing is necessary for compliance with a legal obligation;
d) processing is necessary for the purposes of enforcing the legitimate interests pursued by the Employer or by a third party.

If the envisaged processing is necessary for the purposes of enforcing the legitimate interests pursued by the Employer or by a third party, the organization unit affected by the processing shall contact the Data Protection Officer to identify the legitimate interest of the controller and to perform the balancing test. The envisaged processing may only be

started if it can be established based on the balancing test that the interests of the controller in the processing of data override the rights and freedoms of the Employee or of other persons.

3. Processing of Special Categories of Personal Data

RMC may process special categories of personal data for the purpose defined in the Clause in so far as it is necessary for such purpose, for secondary purposes, for purposes to which the data subject has consented in accordance with Clauses II.2.1 and II.2.2, and to the extent required or allowed by the applicable law.

RMC processes the personal data of Employees related to ***physical or mental health and other data concerning health***, qualifying as special categories of personal data, for the following purposes:

a) administration of pension, social security and health allowances, maternity leave, paternity leave, or other allowances providing rights to the Employees based on their health status;
b) reintegration or support of Employees who are entitled to allowances because of illness or incapacity of work;
c) aptitude tests for certain positions, responsibilities or projects, and decision making in connection therewith (also including aptitude tests upon hiring);
d) providing workplace care for the management of workplace health and safety, health problems or disabilities.

3.1 Legal Basis for the Processing of Special Categories of Personal Data

Special categories of personal data of the Employees may be processed, in particular, on the following basis:

a) on the basis of the explicit consent of the Employee;
b) for performing the obligations of RMC as employer under laws relating to employment and for the exercise of rights, as well as for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, on the basis of Union law or national law, or processing under contract concluded with a health professional (e.g. occupational physician);
c) in cases necessary for establishing, exercising and defending legal claims;
d) in the vital interest of the data subject or any other natural person;
e) in relation to personal data which are manifestly made public by the employee;
f) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law;
g) it is necessary for reasons of public interest in the area of public health;
h) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

If special categories of personal data are processed on the basis of the consent of the data subject, processing may take place upon the prior approval of the Data Protection Officer.

Sensitive data of the data subjects may be processed for Secondary Purposes under the conditions set forth in Clause II.2 in addition to those specified in this Clause.

4. Consent of the Employees

In the absence of the legal bases listed in points a)-c) above, processing of Employee data may be based on the consent of the Employee only in exceptional cases if processing is not closely linked to the employment. Denial of consent shall not entail any adverse legal consequences to the Employee in relation to the employment relationship or other

relationship for work. Before processing on the basis of consent, the organizational unit responsible for the processing shall ask for the opinion of the Data Protection Officer is respect of the envisaged processing. The Data Protection Officer takes measures for investigating the envisaged processing, in particular regarding the consequences of the denial of consent to the Employee.

The Employees are not obliged to give their consent to the processing of their personal data, and they may withdraw their consent any time, but withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Withdrawal of consent shall be possible just as easily as giving consent. If processing takes place explicitly upon the request, initiative of the Employee (e.g. the Employee intends to resort to a service of the Employer not closely linked to the employment or other relationship for work), the Employee's consent to processing, if, prior to initiating the processing, the Employee has received appropriate information regarding the context of processing, shall be considered as given.

Prior to processing on the basis of consent, RMC informs the Employees appropriately in the Employee Privacy Policy. The head of the organizational unit responsible for the processing is responsible for providing such information and for obtaining consent in a documented form.

5. Health Aptitude Tests of Employees and Applicants

Only such declarations and data may be requested from the Employees which do not violate their rights relating to personality and are essential from the point of view of the establishment, performance or termination of employment. The Employees may be subject only to such health aptitude testing that is required by rules applicable to employment, or which is necessary for the exercise of rights and/or compliance with obligations set forth in rules appliable to employment.

The results of the health aptitude test may be disclosed only to the Employee and the professional performing the test. RMC records and processes only the fact of aptitude and sometimes the fact of limitation of limited aptitude in respect of the Employee.

6. Limitations regarding the Processing of Data of Relatives of the Employees

RMC processes the personal data of relatives of the Employees only if

a) it has obtained the relative's personal data with the consent of the relative;
b) processing is necessary for the performance of a contract concluded with the relative;
c) processing is required by law; or
d) it is necessary for compliance with a legal obligation to which RMC is subject.

7. Workplace Control of Employees

Based on legal requirements or its legitimate interest, RMC is obliged to or may control the Employees in relation to their employment. In the course of such inspection of Employees, the employer and the Employee taking part in the inspection shall respect the human dignity and privacy of the Employees under inspection. In connection with workplace inspections the Employees are entitled to the rights under this Policy. The Employees shall be informed of the technical means applied by workplace inspections when establishing the employment relationship.

7.1. Checking Electronic Mails

Based on its legitimate interest in controlling employees as an employer, RMC may check the electronic mails of the Employees by technical means also individually to the extent necessary, in accordance with the principle of graduality, but always taking into account the protection of the private sphere of the Employees.

For the sake of the lawfulness of the checking of electronic mails RMC performs the balancing test under Clause II.18.

If individual checking of electronic mails becomes necessary, the Employer is entitled to view the mails in the e-mail account provided to the Employee for work purposes without limitation, although in accordance with the principles of graduality, primarily by viewing the subject and the addressee. If by checking the subject of the electronic mails RMC does not achieve the goal of the inspection, then after viewing the subject and the addressee RMC may request that the Employee disclose the content of a certain mail or the mail itself. The Employee may request that only an IT security specialist and the Head of Compliance access his/her e-mails only if the right of a third party to secrecy of letters were to be violated by such access. Detailed checks may be carried out only if checks as provided for above are not successful. The Employer is not entitled to access private mails of the Employee.

The manager authorized to represent the company has the right to allow checks.

During the checking the presence of the Employee shall be ensured unless the presence of the Employee would defeat the purpose the checking, it is impossible, or the law allows for the limitation of the rights of the Employee relating to personality. If the Employee is permanently away from work, and it is justified to check his/her e-mail account, the Employee may designate another Employee to access the e-mail account. In the absence of a designated Employee, or if he/she is away from work, the IT specialist responsible for the operation of the system performs this task.

7.2 Checking the Use of Technical Equipment Provided for Work Purposes

Based on its legitimate interest in controlling employees as an employer, RMC may check the use of technical equipment provided for work purposes (e.g. computer, laptop and cell phones). In accordance with the relevant internal rules and instructions the Employer does not allow the private use of technical equipment provided for work purposes; accordingly, the Employees may not store personal content on such equipment. Based on its legitimate interest in the proper use of company assets, the Employer may check the use and contents of devices provided to the Employees.

IT Security personnel are entitled to carry out such checks.

In accordance with the principle of graduality, the primary purpose of the checks shall be the proper use of company equipment. Checks shall not violate human dignity, and the personal life of Employees may not be checked; therefore, the Employer's access during the checks to unnecessary content relating to the Employee and not connected to employment may lead to the application of Employer measures.

During the checking the presence of the Employee shall be ensured unless the presence of the Employee would defeat the purpose the checking, it is impossible, or the law allows for the limitation of the rights of the Employee relating to personality. If the Employee is permanently away from work, and it is justified to check his/her technical devices for personal use, the Employee may designate another Employee in his/her stead. If it can be clearly established that the content found on the device is for official purposes, then such content may be handed over to the Employer. In the absence of a designated Employee, or if he/she is away from work, the IT specialist responsible for the operation of the system performs this task. If the presence of the Employee may be limited, this shall be decided

on by the Head of HR, and the Data Protection Officer shall be informed of such decision prior to the checking. The checking shall not be started until the Data Protection Officer acknowledges such decision, who shall provide feedback on such information without delay, but within 2 workdays the latest.

For the sake of the lawfulness of the checking of technical equipment provided to Employees, RMC performs the balancing test under Clause II.18.

7.3 Camera surveillance

For the purposes of the protection of human life, physical integrity and personal freedom, and of assets, based on its legitimate interest in processing of data, RMC uses camera surveillance at its registered seat and on its premises. The camera surveillance system is operated by RMC.

RMC stores the recordings at the place of their recording and keeps them for a period necessary for the purposes of camera surveillance, thereafter RMC deletes the recordings. In relation to access to, review of, and other circumstances of surveillance, RMC acts in accordance with the provisions of Act CXXXIII of 2005.

For the sake of the lawfulness of camera surveillance based on legitimate interest, RMC performs the balancing test under Clause II.18.

Details on the camera surveillance applied by RMC are to be found in a separate policy.

7.4 Checking Internet Use

Websites visited by Employees, and information recorded and saved during the use of the Internet (e.g. usernames, passwords, etc.) are personal data of the Employees. Based on the legitimate interest of RMC in controlling employees as an employer, IT Security may check the use of the Internet by Employees in accordance herewith.

For the sake of the lawfulness of checking Internet use by Employees, RMC performs the balancing test under Clause II.18.

7.5 Other Ways of Control

Separate policies may be issued regarding other ways of controlling employees, but other ways and means of control shall always comply with the provisions of the Policy, the principle of graduality shall always by observed during the exercise of control to minimize violation of the private sphere of Employees; to this end, adherence to rules by the Employees shall be the primary focus of such control. The organizational unit responsible for the processing in question shall always be responsible for processing of data in the course of the checks, as well as for the compliance of such processing with the requirements of this Policy and of the applicable law.

8. Final Provisions

8.1 Entry into Force

By this Policy entering into force, all previous instructions, rules and procedures regulating data protection activities shall be repealed.

8.2 Organizational Unit Responsible for Maintenance

It is the task of the Data Protection Officer to review and keep the provisions of this Policy up to date.

IV. ANNEXES

Annex No. 1 – Definitions

Processor means a natural or legal person, who processes personal data on behalf of the controller, based on an agreement concluded with the controller and according to its instructions.

Data processing or **processing** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Controller means the natural or legal person, who determines the purposes and means of the processing of personal data.

Personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Archiving means the storage of personal data in a way so that no employees other than the system administrator have access to such data.

EEA or **European Economic Area** means the member states of the European Union, as well as Norway, Iceland, and Liechtenstein.

Priority Interest means the overwhelming interest under this Policy in the case of which an obligation of RMC connected to data protection and the rights of the data subject may be ignored under certain conditions, if the overwhelming interest takes precedence over the right of the data subject to the protection of his/her personal data.

Initial Purpose means the purpose for which the personal data was collected.

Other Purpose means a purpose different from the Initial Purpose and not covered by the concept of Secondary Purpose.

GDPR means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC

Third persons are all natural and legal persons or other entities who or which are not RMC or the data subject.

Legitimate interest means the legitimate (business) interest of RMC or of a third person, preceding the fundamental rights and freedoms of the data subject(s), which is applicable if personal data are processed for a legitimate purpose other than the performance of the contract concluded or to be concluded with the data subject, vital interests of the data subject or of another natural person, or compliance with a legal obligation.

Secondary Purpose means every purpose other than the Initial Purpose, for which personal data are processed.

Employee means the current or ex-employees of RMC, persons applying for a job, and persons undertaking internship by a member of RMC. It means, furthermore, every person who processes personal data within the building of RMC or through its IT system.

National Authority for Data Protection and Freedom of Information or **NAIH** means the Hungarian National Authority for Data Protection and Freedom of Information (1125 Budapest, Szilágyi Erzsébet fasor 22c.).

Personal data or **data** means any information relating to an identified or identifiable natural person.

Special categories of personal data means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Annex. No. 2 – Sample Declaration of Confidentiality

D E C L A R A T I O N

on the obligation of confidentiality in connection with the processing of personal data

I, undersigned _____ (address: _____, place and date of birth: _____) as a person employed by **RMC MedLife Holding Kft.** (registered seat: 1026 Budapest, Gábor Áron utca 74-78. Building A, Floor 3; company registration number: Cg. 01-09-202964) / **RMC MEDICAL Zrt.** (registered seat: 1026 Budapest, Gábor Áron utca 74-78. Building A, Floor 3; company registration number: Cg. 01-10-048721) / **RMC DENTART Kft.** (registered seat: 1026 Budapest, Gábor Áron utca 74-78. Building A, Floor 3; company registration number: Cg.01-09-276010) (**"RMC"**) under a contract of employment / contract for services for the performance of work hereby

d e c l a r e

that I will keep all personal data that I become aware of under the legal relationship with RMC confidential in accordance with the provisions of the law relating to the protection of personal data as in force at all times, and with the Privacy Policy and other Policies of RMC. I will process personal data only for the purpose defined previously by RMC and will not use them for other purposes; I will access them only to the extent necessary in accordance with the "need to know" principle. I hereby acknowledge that my obligation of confidentiality regarding the processing of data will continue to exist without limitation after the termination of my legal relationship.

I have read and understood the Privacy Policy of RMC, and I accept it as binding.

Drawn up in _____, on _____.

Signature: _____ Name:

Organizational unit:

Annex No. 3 – Balancing Test Template

Annex No. 4 – Template for Impact Assessment

Annex No. 4 – Sample Statement of Consent

Statement of Consent to the Processing of Data

I, undersigned _____ (name) (address: _____, place and date of birth: _____, mother's name: _____) hereby declare that I have read and understood the joint Privacy Policy of **RMC MedLife Holding Kft.** (registered seat: 1026 Budapest, Gábor Áron utca 74-78. Building A, Floor 3; company registration number: Cg. 01-09-202964), **RMC MEDICAL Zrt.** (registered seat: 1026 Budapest, Gábor Áron utca 74-78. Building A, Floor 3; company registration number: Cg. 01-10-048721) and **RMC DENTART Kft.** (registered seat: 1026 Budapest, Gábor Áron utca 74-78. Building A, Floor 3; company registration number: Cg.01-09-276010), and in the light of its contents I give my consent to the processing of the following personal data.

I acknowledge that I may withdraw my consent any time without any adverse consequences, and that withdrawal of my consent does not affect the lawfulness of data processing prior to the withdrawal. Based on the provided information I have understood that in some cases the processing of sensitive data is inevitable; therefore, the withdrawal or refusal of my consent may result in the impossibility of the data processing purposes.

Personal data processed:
[•]

Legal basis of processing: Explicit consent of the data subject

Purpose of processing:
[•]

The period for which the personal data will be stored, or the criteria used to determine this period:
[•]

Consequences of failure to provide data:
[•]

Recipients of data transfer:
[•]

Categories of recipients (independent controller, joint controller, processor, person carrying out outsourced activity, other third party):
[•]

_____, _____ 2019

_____
Name: ……

Annex No. 6 – Application Sample for Exercising Data Subject Rights

EMPLOYEE APPLICATION FOR EXERCISING DATA SUBJECT RIGHTS

I hereby request, based on the joint Privacy Policy and employee data protection policy of **RMC MedLife Holding Kft.** (registered seat: 1026 Budapest, Gábor Áron utca 74-78. Building A, Floor 3; company registration number: Cg. 01-09-202964), **RMC MEDICAL Zrt.** (registered seat: 1026 Budapest, Gábor Áron utca 74-78. Building A, Floor 3; company registration number: Cg. 01-10-048721) and **RMC DENTART Kft.** (registered seat: 1026 Budapest, Gábor Áron utca 74-78. Building A, Floor 3; company registration number: Cg.01-09-276010) the following actions to be taken.
(Please mark with an X the actions you request to be taken)

□ exercising the data subject's right of access,

□ exercising the right to erasure ("the right to be forgotten"),

□ exercising the right to rectification,

□ exercising the right of the data subject to restrict processing,

□ exercising the right to object,

□ exercising the right to data portability.

Categories of the personal data affected:

……

……

……

Justification of the request:

……

……

……

Drawn up in _____, on _____

_____
Signature

Name: _____
Address: _____
Phone number: _____
E-mail: _____

Applicant

Date and place of receipt of the application: _____ (signature)
Received on behalf of RMC: _____ (name)

Annex No. 7 – Procedure for Addressing Personal Data Breaches

Process of Addressing Personal Data Breaches

7.1 Detection of a Personal Data Breach

"In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay." (GDPR, Article 33, paragraph (1)).

General rules relating to personal data breaches are set out in Clause 12 hereof.

Personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed. Suspicion of a personal data breach may arise anywhere in the organization, and as the result of compulsory education provided within the organization all Employees shall be able to identify a suspected personal data breach. Notification referring to a personal data breach may be received from any **Employee** and from the **departments of the organization entrusted with tasks connected to security and compliance** (these are the following: IT department).

a. In case it is detected by an **Employee**, the Employee shall notify the Data Protection Officer who – due to his/her broader knowledge in the field of personal data breaches – assists the Employee in deciding whether presumably a personal data breach has occurred, and helps the Employee in making the notification as precisely as possible, in the required format.

b. If the notification comes from any **department of the organization entrusted with tasks connected to security and compliance** (this may be: IT Security, Security Organization), in the course of making the notification the procedure followed in case of business continuity, security, and other events shall be followed, but in the course of the notification process the person or organizational unit responsible for evaluating the event in question shall involve also the Data Protection Officer without undue delay, but within 8 hours after detecting the event the latest.

The suspicion of a personal data breach shall in all cases be registered by the Data Protection Officer in accordance with the principle of accountability, even if he/she considers that no personal data breach has occurred.

7.2. Assessment and Registering of Personal Data Breaches

After the notification the Data Protection Officer shall, with the assistance of the fields concerned, assess the breach and determine the process of addressing the breach, or if the breach does not concern personal data, he/she shall forward it to the competent organizational unit (e.g. Security, IT department). Assessment of the breach shall be carried out within 8 hours the latest after the notification of the breach.

1. All information and evidence used when assessing personal data breaches shall be recorded in the system for registering personal data breaches. In respect of each breach at least the following information shall be recorded:

   a. Circumstances of the notification (date, name and organizational unit of the notifier)
   b. Context of the personal data breach (data subjects concerned and their number, personal data concerned, categories of data subjects concerned, volume of personal data concerned)
   c. Assessment of the personal data breach (presumed consequences and risks to the data subjects concerned)
   d. Plan for addressing the personal data breach (activities for addressing the breach, persons responsible and their achievements)
   e. Measures taken for remedying the personal data breaches (description of technical and organizational measures, their operation in respect of the breach, communication, etc.)
2. In accordance with the principle of accountability, the personal data breach shall be assessed and documented even if the breach has been averted immediately or shortly after the notification.
3. When assessing how to address the personal data breach, the following aspects shall be evaluated:
   a. How personal data are affected
   b. Type of personal data concerned
   c. Context of personal data, possibility of creating a detailed profile
   d. Identifiability of the data subjects
   e. (Expected) effect on data subjects
   f. Technical and organizational measures implemented
4. The final result of the assessment of the personal data breaches in relation of the data subjects may be the following:
   a. The personal data breach presumably does not entail any risk to the rights and freedoms of natural persons.
   b. The personal data breach presumably entails risk to the rights and freedoms of natural persons. (NAIH shall be notified)
   c. The personal data breach presumably entails high risk to the rights and freedoms of natural persons. (NAIH and the data subjects concerned shall be notified)

The following chart serves as a guidance for the assessment of personal data breaches:

It is the task of the Data Protection Officer to maintain the register of personal data breaches, to keep it up to date, and to review it daily.

7.3 Addressing Personal Data Breaches

Personal data breaches shall be addressed by the Data Protection Officer together with the involvement of the IT department. After or meanwhile – if addressing the personal data breach clearly requires assistance from the professional field - assessing the breach, the Data Protection Officer arranges for the involvement of the leaders of the professional fields concerned.

1. Within 4 hours the latest after assessing the breach, the Data Protection Officer arranges for the setting up of an appropriate breach management body and makes a proposal for addressing the breach.
2. The members of the body determine the actions necessary in the short and in the long term for addressing and averting the personal data breach. The breach management body (if the Data Protection Officer has not done it earlier due to lack of information) decides whether it is necessary to notify the National Authority for Data Protection and Freedom of Information and the data subjects affected by the personal data breach, and if necessary, authorizes the Data Protection Officer to prepare communication.

3. It is the task of the Data Protection Officer to arrange for the coordination of the operative breach management activity.
4. It is the task of the Data Protection Officer to arrange for the notification of the data subjects.
5. It is the task of the Data Protection Officer to carry out the tasks after the closing of the personal data breaches, to prepare the records and documentation in connection with the breaches, to arrange for the re-channeling of the lessons learned from the breaches, and to prepare the necessary training or educational material.
6. The Data Protection Officer shall record the tasks emerging in case of personal data breaches in the internal system and shall arrange for the monitoring of their performance.
7. If the personal data breach results / may result in operational risk loss, and/or operational risk measures are necessary, the Data Protection Officer shall report it in writing to the Managing Director for Corporate Governance without undue delay.