Privacy and Personal Data Protection Policy

Introduction

The company **ΜΙΝΕ ΔΙΑΧΕΙΡΙΣΤΙΚΗ ΛΙΜΙΤΕΔ (MINE DIACHIRISTIKI LIMITED)** with registration number HE 321545, which is the owner of the private hospital, with the name 'Evangelismos Private Hospital' and which operates connected outpatient / blood collection points in Paphos district (hereinafter called the 'Company', or 'Evangelismos', or through personal pronouns on first plural like 'we' or through possessive pronoun on first plural like 'our', as well as respective expressions), gives much attention to your personal data protection, to the security and the protection of your privacy, when it is collecting and processing information about you. The present policy aims to inform you about the collection, processing, preservation and saving of Personal Data, the ways they can be used and transmitted, the protection measures the Company takes to protect them, the reasons and the kind of data collected, your rights as an individual, providing you the necessary information for your full awareness in accordance with the institutional frame work.

We assure you, that the present protection of Privacy and Personal Data Protection Policy (hereafter called the 'Policy') complies with and respect the European Regulation for Personal Data Protection EU 2016/679 (hereafter called the 'Regulation'), the related harmonizing legislation L.125/I/2018 of the Republic of Cyprus, as well as the instructions, recommendations and guidelines of the Commissioner of Personal Data Protection.

Useful Definitions

Personal Data (referred also with the acronym 'PD'): Each information referring to a person and identifies it or it can identify it, like, indicatively but without limitation, online full name, I.D. number, contact details, location, online data, as well as data which are related to its physical, genetic, psychological or financial situation. The person (natural person), in which these data are referring and or concern, is called **'Data Subject'**.

Violation of Personal Data: The violation of security, which leads to accidental or unlawful destruction, loss, alternation, disclosure or share, unauthorized access and similar actions.

Controller: The natural or legal person, or the public authority, or other agency, or other body which determines the purposes and the way or the means of processing personal data.

Processor: A natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller.

Process of Personal Data: Every action or sequence of actions, which is relevant to personal data, like, indicatively but without limitation, the collection, submission, organisation, structure, storage, adaptation, alternation, retrieval, change, search, use, disclosure, dissemination or any other form of disposal, the association, combination, restriction, deletion and destruction.

Third Party: Any natural or legal person, other than the Data Subject, the Controller, the Processor and persons who, under the direct authority of the Controller or Processor, are authorised to process personal data.

The Controller

In cases we act as Controller, i.e. when we define the purpose and the means of processing in the sense of the above mention definition, the Controller is our company, the legal person MINE ΔΙΑΧΕΙΡΙΣΤΙΚΗ ΛΙΜΙΤΕΔ (MINE DIACHIRISTIKI LIMITED) with registration number HE 321545 (address 87, Vas. Konstantinou, 8021 Paphos, Cyprus tel +357 26848000, email: info@evangelismos.com.cy).

Principles we serve

At **Evangelismos**, we commit to apply the following principles for the processing of the Data Protection (called also 'PD' as above mentioned) according to article 5 of the Regulation:

- Legality, objectivity and transparency – PD are submitted to lawful and legitimate processing in a transparent way.
- Purpose limitation – PD are collected for specified, explicit and legitimate purposes and are not further processed, in incompatible ways to these purposes.
- Data Minimisation – PD are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accuracy & Quality of Data – PD are accurate and kept up to date as soon as the Company is aware of such change.
- Storage Limitation – PD are kept for no longer than is necessary and not for longer or for the time required for any applicable law.
- Integrity and Confidentiality – We use the technical and organizational measures to guarantee as far as possible the security of your PD, especially, indicative but without limitation, protection against unauthorised or unlawful processing and against accidental loss or destruction or damage.
- Finally, we can prove our compliance with the above Principles in application of the Principle of Accountability, as required by the Regulation.

Collection of Personal Data

As a Controller, we collect data about you, in the following cases:

- When you contact us directly or by telephone or indirectly, for example, through our website and email, or affiliates, or social media, to get informed about our services or ask us about our services.
- When you contact us for you or third party to receive medical services, when we provide medical services to you or an accompanying person, when you work with us as a professional associate, or when you participate directly or indirectly in works and activities related to the provision of our services.

- When you fill out one of our forms in written or electronic form, or submit a complaint to us.
- When your data is disclosed to us by professional partners with your consent or in case of need.
- When you are connected to our webpage, or when you visit our premises where a video surveillance system operates legally for security reasons.
- When you apply for work to our Company.
- When our Company employees you.

Furthermore, it is noted that we process PD which third parties disclose to us, in which case we act as Processors on their behalf. In this case, responsible to inform you accordingly are these third parties.

Personal Data of Minors

We collect as Controllers personal information related to minors, only with verifiable parental consent, in cases we can check it. For example, it's not possible to check this information, which are notified to us without physical presence.

Personal Data which we may collect as Controllers

Information from the following data categories related to you, may be collected and processed, per case, when they serve the purpose of their collection and in accordance with the appropriate legal basis:

- Your contact information or of the person you indicate (full name, address, telephone or fax number, email)
- Professional Status (occupation or job position)
- Identification data such as, indicatively but not limited, ID number, passport number, residence permit number and social security number,
- Information of contracting parties, such as necessary information from the above mentioned information, terms and amounts.
- Information about and in relation with your medical condition like, indicatively but without limitation, age and/or birth date, pre – existing deceases and medical history, history of allergies, medication you take, habits that affect health, symptoms, evaluation of critical points, diagnosis, examinations deemed necessary, information of treating doctor, details of previous contacts, details of treatments and care required, health data from medical services not provided by us but reported to us by you or by others, nutritional issues and the outcome at the time discharge, including any information necessary to be recorded under the applicable legislation.
- Authorizations regarding the provision of services to related persons, or for the sending of information to third parties, natural or legal persons.
- With your explicit consent or that of the person accompanying you, in the case that you are unable to obtain personal consent, we may photograph data of medical interest such as

rashes, wounds, sores, ulcers and the like, for the purpose of comparative medical evaluation or the progress of your health.

- Payment information (IBAN or account number, tax registration number, desired payment method, credit card details depending on the method of payment, payment terms, depositors details, etc.).
- Information of accidents or incidents, such as information of persons involved and witnesses, evidence and relevant information during the investigation.
- Customer history (satisfaction, transactions, complaints, terms) and evaluation data of persons and situations.
- Applications Data / websites / social media (only necessary cookies, full name or nickname, photo, public information and comments when contacting us on social media, or attachments to emails)
- Your image when, with your consent, it appears in our social media accounts that we maintain on our website or when you visit our facilities where a recording system (video surveillance) operates for security reasons.
- The data mentioned in your CV such as studies, previous job experiences and skills or any attached documents that you send us.

It is noted that, for the employees of the Company, other personal data are obtained, for which they are informed through documents, manuals, policies and procedures and information that takes place internally in the Company.

Purposes of processing – Legal Bases of Personal Data processing

The processing of personal data is based on or at least one of 'the legal bases', as referred to article 6 of the Regulation, as well as to the article 9 of the Regulation for the processing of special categories of PD. Legal bases, on which the collection and the processing of PD is based, are, indicatively but without limitation, (a) consent, (b) compliance with commitments to fulfil our contractual obligations, (c) compliance with our legal obligations, (d) the processing necessary for the safeguard of your vital interests or of another natural person and (e) safeguarding our legitimate interests. Respectively, regarding the special categories of personal data, legal bases are, indicatively but without limitation, (a) consent, (b) execution of obligations and exercise of specific rights of controller or data subject, in the field of labour and social security and protection law, (c) where treatment is necessary for the purposes of preventive or occupational medicine, assessment of the employee's ability to work, medical diagnosis, provision of health or social care treatment.

The legal basis on which personal data processing is based, relates to each processing purpose as follows:

Consent: When you contact us in any way, directly or indirectly, as interested in our services, when you are interested in working or working with us, when filling out forms, when you complain, when

you visit our social media accounts, when you explicitly and freely consent to take a photo, when you give us your business card.

Fulfilment of our contractual obligations: When you receive services from us, when you work or cooperate with us, when paying our obligations or when we communicate with you under contracts.

Compliance with our legal obligations: When complying with our obligations under the applicable law, when complying with the competent authorities, respectively, like, indicatively without limitation, the competent authorities for medical matters and the provision of medical services, for matters of labour law, regulatory or tax authorities, prosecutors and judicial authorities.

Safeguarding your vital interests: Indicatively but without limitation, in relation to the achievement of medical diagnosis, prevention and treatment.

Safeguarding our legitimate interests: For improving our services, managing of accidents, for our payment, for evaluating persons and situations, as well as for the recoding of your image by the video surveillance system that we operate in accordance with the law and the instructions/ Guidelines of the Office of the Personal Data Commissioner.

Informing of our staff about the legal bases of processing related to personal data that we collect from them, is done internally, indicatively but without limitation, through documents and manuals as well as through staff training (training of departments heads / departments heads based on the updated, from time to time, organizational chart of the Company).

Keeping your data

We storage your PD for as long as needed for the register processing purpose as well as for any other permitted related purpose.

The data collected on the basis of our contractual and legal obligations, are retained after the expiration of the contractual and legal obligations as provided by the respective institutional framework.

Data that may by needed for our legal rights as Controller, are kept until the reason of keeping them ceases or until the limitation of the related rights expire, respectively.

Especially for the data which we are processing based on your consent, these are kept from the time of obtaining of the relevant consent until this is revoked.

For Cookies, you can be informed for the relevant policy by clicking here.

Your CV, if you send it as candidates for work, as well as relevant information are kept for 12 months.

The personal data of the system CCTV, which legally operates based the instructions / guidelines of the Office of Personal Data Commissioner, are kept for 15 days.

Information which are no longer necessary, are safely destroyed or anonymized. We restrict access to your data to persons who need to process such information for the purpose for which it was collected.

The security of your data

We have taken reasonable organizational and technical measures, to protect the information we processing and especially, the special categories of personal data. We follow international standards and practices to ensure the security of our networks. We ensure that your personal data are processed securely and legally, in accordance with policies, as well as with the development and application of processes. For example, the following security measures are used for the protection of personal data against misuse or against any other form of unauthorized processing:

- The access to the personal data is limited to certain number of authorised employees, for specific purposes and the necessary transaction of data is done with safe procedures.
- Pseudonymization of data is used, where is possible, during certain processes.
- Our staff, commits with confidentiality rules, having graded and limited access to only necessary data. On special categories of PD, access is given to staff in a completely restrictive way and pseudonymization is applied where this is possible.
- We choose reliable partners, who commit in writing according to the article 28 of the Regulation, with the same obligations, regarding to the protection of personal data. We also reserve our right to control them according to the article 28, paragraph 3, item h.
- In our IT system which is used for the processing of personal data, appropriate technical measures are taken in order to prevent loss, unauthorized access or other processing of personal data.

Moreover, the access to the said IT systems, is monitored on an ongoing basis to detect and prevent illegal use at an early stage. Although data transition through internet or a webpage cannot be protected on a guaranteed level from cyberattacks, we are working to keep physical, electronical and procedurally safety measures for the protection of your data.

Some of the safety measures which the Company takes are not announced for obvious reasons.

To whom your data can be disclosed

We are taking all measures, so that the recipients of personal data to be as less as possible per case. The personal data we are collecting and processing as Controllers, are, mainly, being processed by the authorized personnel of the Company and are disclosed to third parties, only when the lawfulness of such notify is fully justified and that such parties apply respective lawful and appropriate processing practices.

For specific data, which we are legally processing as Controller, access may have (or may be notified) depending on each case:

- Any competent supervisory or prosecuting authority, in the context of its role.
- Any other public or judicial authority, if required by law or court order.
- The company that operates as an external partner – administrator the medical programme (IT administrator) under an appropriate agreement, as referred to a subsequent point.

- The auditor of the Company, for any required financial data, under confidentiality.
- The legal consultant, for any required legal data, under confidentiality.
- After your direct or indirect order, your personal data can be disclosed to third parties (for example other doctor of your selection) or other collaborating insurance companies and only for the necessary part of information.
- Collaborating Banks (Of the Company, the customers, the staff or of the partners and suppliers) only for data relating to payment issues.
- The system consultants we keep, the Certification Body for system compliance, the trainer and the HRDA for training matters and only for the necessary parts of information.

The above third parties except the Authorities, are contractually committed with the Company that they will use the personal data only for the above, respectively, reasons, that they will not transmit this personal information to other third parties, as well as they will not notify it to third persons, unless the law or Court decision imposes it.

Place of processing – Transition to third countries

The personal data we collect, are being processed mainly within the European Economic Area (EEA). The only procession which takes place to Third country, is the accessibility of the administrator (IT administrator) of the specialized Hospital Information software we use, with whom we collaborate. This administrator is the creator of this specialized software and has the role of administrator for maintenance and troubleshooting purposes. This processing is subject to appropriate guarantees based on Article 46, having signed with this Administrator the Standard Contractual Clauses required under the applicable legal framework.

Your rights as data subject and how you can exercise them

You have the right of:

- Information,
- consent (when receiving / taking personal data is based on consent),
- access to the personal data concerning you,
- correction (in order to correct any deficiencies or inaccuracies in the data),
- deletion of your personal data (as long as and in the cases that such right can be satisfied as mentioned below),
- processing restriction,
- opposition to processing,
- data portability,
- objection.

Its underlined, that the Company does not use automated decision-making tools, including profiling.

If personal data processing is based on your consent, you can recall such consent any time, by contacting us.

Your right of information is exercised with the posting of this policy, or furthermore in some cases, by providing relevant information on how you can be informed, via written forms with which we can communicate with you. You can request our policy in printed form by contacting us.

Your right of information with regards to the video surveillance system (CCTV), which legally operates with image recording for the safety of people and property, is exercised with the existence of appropriate informative boards before you enter the range of the recording area. Additional information (level b' information) can be requested from the reception of the hospital.

Your right to consent is provided, by design and by definition, in any case required.

At the same time, you have the following additional rights, provided you exercise them directly or through legal representation in writing and after it has been confirmed that you are the data subject:

Right of Access: You have the right to be informed about which data we keep for you, for the process of your data by us, as well as you have the right of access to the data that concern you.

Right of Correction: You have the right to request correction or completion of your data, whether these are inaccurate or incomplete.

Note: Given, that it is not possible to know any change of your personal data if you do not inform us, please help us keep accurate and updated information about you via informing us about any changes of your personal data.

Deletion Right: You have the right to request the deletion of your data.

We can satisfy this right if:

- The data are no longer necessary for the purposes for which they were collected.
- If there is no other legal basis for processing, except the consent.
- If you exercise the right of opposition (see with regards to this right below)
- If the data are processed contrary to the current legislation.
- If the data were collected in the framework of the Information of Society, when you were minor.

We reserve the right to refuse to satisfy the above right for any period required, if the process is necessary in order to abide with our legal or contractual obligation, for reasons of public interest, or for the establishment, exercise or support of our legal claims. (article 17§3 of the Regulation).

Procession Restriction Right: You have the right to point out the data, aiming their restriction of process, when:

- You are doubting their accuracy for the period you require us to check their accuracy.
- The process was unlawful and instead of deletion, you ask the restriction of their process.
- We do not need them for the purposes they were collected, but you need them to support your legal rights.
- You are doubting the process and until it is established if our legal rights supersede yours.

Portability Right: You have the right to receive your data in a structured, commonly used and machine-readable format, as well as to request their transfer, both to you and to another person duly authorised by you to process them.

Opposition Right: You have the right of opposition any time during process, including profiling, as well as when the reason for processing concerns direct marketing.

We also inform you that, we do not use automated decision-making tools including profiling.

All the above apply in the case we act as a Controller. For the cases we act as Processor, qualified for informing you, as well as for handling your requests, is the controller of these rights.

Our Company, in case you submit any relevant in writing request, will consider your request and respond to you within one month of receipt either for its satisfaction, or to inform you with regards to the objective reasons that prevent the satisfaction of your request, or, considering any potential complexity of the request and the number of requests at that time and any similar restraining factors, to request an extension to reply, for up to 2 (two) months (Article 12§3 of the Regulation).

The exercise of our rights above, is carried out free of charge for you, by sending a relevant application, or letter, or email, to our Company or to the Data Protection Officer mentioned below. The abusive exercise of the above rights (Article 12§5 of the Regulation), can impose the payment of reasonable fee.

In case you are not satisfied with the use of your data from us, or from our response for the exercise of your above rights, you can submit a complaint with the competent authority of the Republic of Cyprus, i.e. at the Office of the Commissioner for the Personal Data Protection.

Breach of Personal Data

In case of breach of security and integrity of personal data which are at our disposal and concern personal data for which Controller is our Company, we will take the following measures (according to articles 33 and 34 of the Regulation):

- We will review, evaluate and implement the procedures required to limit the breach.
- We will evaluate the risk and its impact on the rights and freedoms of data subjects.
- We will try to reduce the damage that has been or may be caused as much as possible.
- We will notify, within 72 hours of being notified of the breach, the Office of the Commissioner for the Personal Data Protection , if necessary (or on short time the Controller if we act as a Processor).
- We will evaluate the impact on your privacy and take appropriate action to prevent the recurrence of the breach.

In case we act as a Processor we will inform the Controller as soon as possible.

Links with other Websites

Our website may contain links to other websites that are not operated or controlled by us. If you click on a third party link, you will be directed to that third party website. We recommend that you check the Privacy Policy for each website you visit. We do not have the control and we do not take any responsibility for the contents, privacy policies, or practices of any third party websites or services.

Contact Information of Personal Data Commissioner

Office of the Commissioner for the Personal Data Protection, 1 Iasonos, 1082 Nicosia, telephone +357.22818456, email: commissioner@dataprotection.gov.cy.

More information and terminology for the Regulation, you can find in webpage https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A32016R0679.

Contact information of the Controller

If you want to contact us, for any matter with regards to your personal data, or to exercise any of your rights, you can contact our Company or directly the Data Protection Officer, Mr. Konstantinos Michail Lawyer, on telephone +357 26 080980 (office working hours), or fax +357 26 080989, or email dpo1@evangelismos.com.cy.

Policy update

The present policy has been revised on 26th of February 2021 and can be revised again if there is any significant change. This revise will be available in our website, with a note of the date it applies. You can find hardcopy of the present in our facilities or this can be sent to you upon request.