Privacy and Personal Data Protection Policy

Introduction

The company MINE 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 means any information relating to an identified or identifiable natural person ('**data subject**'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as (indicatively) a name, an identification number, age, permanent address and contact details, occupation, bank details, education, work, an identifier related to information and communication technologies such as Internet Protocol address etc., or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Processing means any operation or set of operations which is performed on information and/or personal data or on sets of personal data, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

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

Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Third party means a natural or legal person, public authority, agency or body 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.

Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Confidentiality means a characteristic of the information by which it is available only to authorised persons or systems.

Integrity means a characteristic of the information by which it is changed only by authorised persons or systems in an allowed way.

Availability means a characteristic of the information by which it can be accessed by authorised persons when it is needed.

The Controller

In cases we act as the 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 adhere to

At Evangelismos hospital, we are committed to, and adhering to, the following principles of processing personal data in accordance with Article 5 of the Regulation. The personal data is:

- processed lawfully, fairly and in a transparent manner in relation to the data subject (**principle of 'lawfulness, fairness and transparency'**);
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (**principle of 'purpose limitation'**);
- adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed (**principle of 'data minimisation'**);
- accurate and, where necessary, kept up to date; we take every reasonable step to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, erased or rectified without delay (**principle of 'accuracy'**);

- kept in a form which permits identification of data subjects for no longer than it is necessary or as required by relevant Laws (**principle of 'storage limitation'**);
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organisational measures (**principle of 'integrity and confidentiality'**).

Finally, we are able to demonstrate compliance with the aforementioned principles (**principle of 'accountability'**).

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 directly or through a 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 Personal Data 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 the Controller

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 at least one of 'the legal bases', as referred to article 6 of the Regulation. Legal bases, on which the collection and the processing of Personal Data is based, are:

- your consent (Article 6.1.a) or explicit consent (Article 9.2.a) in case of special categories of personal data;
- processing that is necessary for the performance of a contract to which you as the data subject is party, or in order to take steps at your request as the data subject prior to entering into a contract (Article 6.1.b);
- the compliance with our legal and statutory obligations (Article 6.1.c);
- the safeguarding of our legitimate interests, except where such interests are overridden by the interests or fundamental rights and freedoms of yours as the data subject (Article 6.1.f).
- Under specific circumstances we may process personal data when processing is necessary in order to protect the vital interests of you as the data subject or of another natural person.

Respectively, regarding the special categories of personal data, legal bases usually are:

- your explicit consent,
- when processing is necessary for the purposes of carrying out our obligations and exercising specific rights of us as the controller or of you as the data subject in the field of employment and social security and social protection law,
- when processing is necessary to protect the vital interests of you as the data subject or of another natural person where the data subject is physically or legally incapable of giving consent
- when processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services.

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 cooperating 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.

Processing based on a contract: 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: to comply with our legal obligations to all sorts of authorities such as health and medical authorities, labour law, regulatory authorities, tax, accounting, auditing, judicial authorities and agencies or in connection with our contractual obligations or during payment of our liabilities.

Safeguarding our legitimate interests: to improve our services, or when investigating and managing any potential incident, to receive our payment, or for the assessment of persons and situations. In this specific legal basis is also based the CCTV operation in our premises that we operate for the protection of people and the property.

Our employees are informed internally about the processing purposes and the legal bases under specific documents.

Retention of Data

We store personal data for as long as it is required by the respective processing purpose and any other permitted linked purpose.

Data collected on the basis of contractual and legal obligations shall be retained after the expiry of the contractual and legal obligations as provided by the relevant institutional framework.

Data that may be needed for our legitimate interests as a Controller shall be kept until the reason for storing such data ceases.

Specifically, the data we process based on your consent, is kept from obtaining the consent until it is revoked or there is no longer need to store it.

Personal data you disclose to us as candidates are stored for 12 months or until you revoke your consent regarding processing of these data.

The CCTV recording is maintained for 15 days and then it is anonymised by overwrite.

Information that is no longer necessary is securely destroyed or anonymised. We limit access to your personal data to those employees who need to use it for the specific purpose.

The security of your data

We have received reasonable organisational and technical measures to protect the personal data we collect and process, and in particular any specific categories of personal data. We follow international standards like the ISO 27001 Standard and practices, to ensure the security of our operations. We ensure you that your personal data is processed securely and legally, by adhering to policies and developing and implementing procedures in accordance with the purposes and legal bases of processing. For example, the following security measures are used to protect personal data against unauthorised use or any other form of unauthorised processing:

Access to personal data is restricted to a limited number of authorised employees under a need-to-know basis, and the necessary data transfer is done by secure procedures. Encryption and Pseudonymization of data is used, where is possible, during certain processes.

Our employees are bound to confidentiality rules and agreements, with limited classified access to the necessary data only.

We select trusted collaborators who are committed in writing, in accordance with Article 28 of the Regulation, to the same obligations regarding the protection of personal data. We reserve the right to audit them in accordance with Article 28 (3) (h).

In our ICT (Information and Communication Technologies) systems used for the processing of personal data, all technical measures are taken to prevent loss, unauthorised access or other illegal processing.

In addition, access to these ICT systems is monitored on a permanent basis in order to detect and prevent illegal use at an early stage. Although the transfer of data through the Internet or a web site cannot be guaranteed to be protected from cyberattacks, we work to maintain physical, electronic and procedural security measures to protect your data.

Some of the security measures we take are not announced for obvious reasons.

To whom your data may be disclosed

We take measures to ensure that the recipients of personal data we process as the Controller are kept to a minimum. The personal data we collect is disclosed to third parties, provided that the legality of such disclosure is fully justified. Such processing by third parties is usually view only, and only under specific circumstances may include the retention of such data by the 3rd party – recipient, especially in relation to authorities, or during legal cases, or payments, or incidents' investigation. Specific personal data from those we lawfully collect as a Controller, may be accessed (or disclosed) on a case-by-case basis by:

Any relating supervisory authority within its role;

Any public or judicial authority where required by law or judicial decision.

The auditor of the company, for necessary data required to fulfil the audit (financial, employment, contracts and other controls), under confidentiality.

The company that operates as an external partner – administrator the medical programme (IT administrator) under an appropriate agreement, as referred to a subsequent point.

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.

The legal advocate, for whatever data is required in legal cases, under confidentiality.

The Insurance cooperating company and only for the relevant part of the information.

Partner banks (of the company, the staff or affiliates and suppliers), only for payment related data.

The training or systems consultants, for training or systems control issues and only for the necessary pieces of information and data under confidentiality agreements.

The Certification Body during their audits.

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.

Territorial Scope – Transfer to third countries

The personal data we collect is processed within the European Economic Area (EEA) and/or an adequacy decision area according Article 45.

The only procession which takes place to Third country, is the accessibility by the IT administrator in data of the specific Hospital management software we use under the required Standard Contractual Clauses that are defined by the European Data Protection Board. This administrator is the creator of this specific 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 to be informed, the right of consent when this is the legal basis of data collection and processing, the right of access to your personal data, the rights of rectification and erasure (in cases it is permitted), the right to restriction of processing, the right to data portability, the right to object. If processing is based on your consent, you may withdraw it at any time.

The **right to be informed** is exercised through this privacy and personal data protection notification. In some cases, it is also mentioned in documents – forms we are using.

We inform you that we are not using software of decision making solely based on automated processing including profiling.

The **right of consent** is provided by design as we have reviewed all processing activities and ask your consent when the case.

Right of access: you have the right to obtain from us confirmation as to whether or not your personal data is being processed as well as other relevant information, and, where that is the case, access to your personal data.

Right of rectification: you have the right of rectification of your inaccurate personal data as well as to have incomplete personal data completed by providing a supplementary statement.

Note: Since it is not possible for us to be aware of any changes to your personal data if you do not inform us, please help us keep your information accurate by informing us of any changes to your personal information we do process.

Right to erasure ('right to be forgotten'); we have to answer such right when:

- your personal data is no longer necessary in relation to the purposes for which we collected it;
- withdraw your consent on which the processing is based and where there is no other legal basis for the processing;
- your personal data has been unlawfully processed;
- your personal data has to be erased for compliance with a legal obligation we are subject to;
- your personal data has been collected in relation to the offer of information society services.

We reserve the right to refuse this right if the processing is necessary for compliance with any legal obligation, we are subject to, or for reasons of public interest, or for the foundation and exercise or support of our legal claims (according to Article 17 § 3).

Right to restriction of processing; you have the right to restriction of processing when:

- you contest the accuracy of your personal data for a period enabling us to verify the accuracy of the personal data;
- the processing is unlawful and you oppose the erasure of the personal data and request the restriction of their use instead;
- we no longer need your personal data for the purposes of the processing, but it is required by you for the establishment, exercise or defence of legal claims;
- you objected to processing pending the verification whether our legitimate grounds override those of yours.

Right to data portability: You have the right to receive your data in a structured, commonly used and machine-readable format and under an explicit request such data to be transferred to both you and another natural or legal person who will process it when:

- the processing is based on consent or the data were processed for the performance of a contract to which you were a party; and
- the processing is carried out by automated means.

Right to object: you have the right to object to the processing of your data at any time when the reason for the processing relates to direct marketing.

In the event that you make such request in a written or electronic form regarding any of the above rights, we will assess your request and respond within one month of its receipt, either for its satisfaction or to provide you with objective reasons preventing it from being satisfied, or, given the complexity of the request and the number of requests at the given time, request an extension of response for a further up to two months period (according to Article 12.3 of the Regulation).

The exercise of your rights is free of charge. Where requests from you are manifestly unfounded or excessive, in particular because of their repetitive character, we may refuse to answer or charge you an administrative fee.

If you are dissatisfied with the use of your data by us, or our response after exercising your rights, you have the right to lodge a complaint with a supervisory authority.

Breach of Personal Data

In the event of a breach of the security and integrity of the personal data processed, we will take the following measures (in accordance with Article 33 and 34 of the Regulation in case we are the Controller) and we will:

- Assess it in order to implement the appropriate procedures needed to limit the breach;
- Examine the extent of the breach and the sensitivity of the data included;
- Evaluate the risk and its impact on your rights and freedoms;
- Endeavour to reduce as much as possible the damage that is or may be caused;
- Notify within a time limit of 72 hours of becoming aware of the breach, the National Personal

Data Protection Authority, if required;
- Assess the impact on your privacy and take appropriate measures to prevent the repeating of the incident.

In the event we are the 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 site. We recommend that you review the Privacy Policy for each site you visit. We have no control over and assume no responsibility for the content, privacy policies, or practices of any third-party sites or services.

Contact details with the National Data Protection Authority

Office of the Commissioner for the Personal Data Protection, 15 Kipranoros, 1061 Nicosia, telephone

+357.22818456, email: commissioner@dataprotection.gov.cy.

More information and terminology for the Regulation, you can find in webpage https://eurlex.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 15th of June 2023 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.