GENERAL PERSONAL DATA PROTECTION POLICY

Version 1.0 – September 2022

This policy sets out the overall framework of data processing activities of magicmedical.de (hereafter “MAGIC MEDICAL”).

Scope, Purpose, and Users

MAGIC MEDICAL strives to comply with applicable laws and regulations related to Personal Data protection in countries where MAGIC MEDICAL operates. This Policy sets forth the basic principles by which MAGIC MEDICAL processes the personal data of clients, suppliers, employees and other individuals , and indicates the responsibilities of its business departments and employees while processing personal data.

This Policy applies to MAGIC MEDICAL and its third parties processing the personal data of data subjects.

The users of this document are all employees, permanent or temporary, and all contractors working on behalf of MAGIC MEDICAL.

Reference Documents

EU GDPR 2016/679 (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)
The Turkish Data Protection Law no. 6698
Employee Personal Data Protection Policy
General Data Protection Notice
Data Retention Policy
Data Protection Impact Assessment Guidelines
Information Security Policy
Breach Notification Procedure

Definitions

The following definitions of terms used in this document are drawn from Article 4 of the European Union’s General Data Protection Regulation:

Personal Data: Any information relating to an identified or identifiable natural person ("Data Subject") who can be identified, directly or indirectly, from such data, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the Data Subject.

Sensitive Personal Data: Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms of the data subject. Those personal data include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning the data subject’s sex life or sexual orientation.

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

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

Processing: An 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, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of the data.

Anonymisation: Irreversibly de-identifying personal data such that the person cannot be identified by using reasonable time, cost, and technology either by the controller or by any other person to identify that

individual. The personal data processing principles do not apply to anonymized data as it is no longer personal data.

Pseudonymisation: 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. Pseudonymisation reduces, but does not completely eliminate, the ability to link personal data to a data subject. Because pseudonymised data is still personal data, the processing of pseudonymised data should comply with the Personal Data Processing principles.

Supervisory Authority: An independent public authority which is established by a Member State pursuant to Article 51 of the EU GDPR.

Basic Principles Regarding Personal Data Processing

The data protection principles outline the basic responsibilities for organisations handling personal data. Article 5(2) of the GDPR stipulates that "the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

4.1 Lawfulness, Fairness and Transparency

We will only process personal data where we have one of the following 'lawful bases' (legal reasons) to do so under data protection law:

The data needs to be processed so that MAGIC MEDICAL can fulfil a contract with the individual , i.e. we need the data in order to carry out your instructions , or the individual has asked MAGIC MEDICAL to take specific steps before entering into a contract

The data needs to be processed so that MAGIC MEDICAL can comply with a legal obligation, in particular legal requirements stemming from the Decree Law No. 663, which is the main legislation establishing us as a legal entity.

The data needs to be processed for the legitimate interests of MAGIC MEDICAL or a third party (provided the individual's rights and freedoms are not overridden)

The individual has freely given clear consent

4.2 Purpose Limitation

We will only collect personal data for specified, explicit and legitimate reasons. We explain these reasons to the individuals when we first collect their data as per the General Data Protection (or Privacy) Notice.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

MAGIC MEDICAL staff will only process personal data where it is necessary in order to do their jobs. When staff no longer need the personal data they hold , they will ensure it is deleted or anonymised or encrypted so as to make it inaccessible . This will be done in accordance with MAGIC MEDICAL's Data Retention Policy.

4.3 Data Minimization

All Personal data processed is adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. MAGIC MEDICAL may apply anonymization or pseudonymisation to personal data if possible to reduce the risks to the data subjects concerned.

4.4 Accuracy

All Personal data processed is accurate and, where necessary, kept up to date; reasonable steps are taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified in a timely manner.

4.5 Storage Period Limitation

Personal data will be kept for no longer than is necessary for the purposes for which the personal data is processed (or will be anonymised or pseuonymised so that it cannot be used to identify the individual or encrypted so as not to be accessible). This can be referenced in our Data Retention Policy.

4.6 Integrity and confidentiality

Taking into account the state of technology and other available security measures, the implementation cost, and likelihood and severity of personal data risks , MAGIC MEDICALapplies appropriate technical and organizational measures to process Personal Data in a manner that ensures appropriate security of personal data, including protection against accidental or unlawful destruction, loss, alteration, unauthorized access to, or disclosure.
We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law
Completing privacy impact assessments where MAGIC MEDICAL processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
Integrating data protection into internal documents including this policy, any related policies and privacy notices
Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
Maintaining records of our processing activities, including:
For the benefit of data subjects, making available the name and contact details of
MAGIC MEDICAL and all information we are required to share about how we use and process their personal data (via our Data Protection notices)
For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure
4.7 Accountability

MAGIC MEDICAL, as a Data Controller, is responsible for and is able to demonstrate compliance with the principles outlined above.

Building Data Protection in Business Activities
In order to demonstrate compliance with the principles of data protection, MAGIC MEDICALhas built data protection into its business activities.

5.1 Notification to Data Subjects

(See the Fair Processing Guidelines section 6.1)

5.2 Data Subject’s Choice and Consent

(See the Fair Processing Guidelines section 6.2)

5.3 Collection

MAGIC MEDICAL strives to collect the least amount of personal data possible. If personal data is collected from a third party, we will ensure that the personal data is collected lawfully. We collect and use your personal data to

administer our relationship with you, including to respond to your enquiries or complaints, to provide our Services to you, to manage our Contracts with you, to inform you about other services, the partners, promotions and events, to administer and improve our Website and Services, to respond to requests from authorities, to comply with our contractual and legal obligations, and for other legitimate business purposes. MAGIC MEDICAL does not share, sell, rent or trade personal data with third parties for promotional purposes.
When you express an interest in obtaining additional information about the Services or registering for an event, you provide MAGIC MEDICALwith personal contact information, such as name, company name, address, phone number, and email address to contact you. In addition, when you purchase the Services or are registered for an event, MAGIC MEDICALmay also require you to provide the Company with means for financial qualification and billing information, such as billing name and address, and the number of employees within the organization that will be using the Services which is not considered personal data.

We may ask you for information to enable us to provide a Service to you and we collect this information either in person or by telephone, written/digital correspondence or via the website. Subject to your consent where required by law, we use cookies and other technologies to track the use of our websites and services.

Subject to your consent where required by law, we may use your personal data to conduct marketing, promotional and informational activities and to perform business analytics, satisfaction surveys or market research and conduct direct marketing.

We may share your personal data with third party providers that we engage to process data on our behalf, when such sharing is required by law or other situations as permitted by law. In accordance with applicable law, you have the right to access personal data we hold about you, to rectify, delete or erase inaccurate data, to object, at any time and free of charge, to the processing of your personal data for direct marketing purposes, as well other rights under applicable law.

5.4 Use, Retention, and Disposal

The purposes, methods, storage limitation and retention period of personal data are consistent with the information contained in the General Data Protection Notice. MAGIC MEDICAL will maintain the accuracy, integrity, confidentiality and relevance of personal data based on the processing purpose. Adequate security mechanisms designed to protect personal data are used to prevent personal data from being stolen, misused, or abused, and to prevent personal data breaches.

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage. In particular:

Paper-based records that contain personal data are kept under lock and key when not in use
Portable electronic devices, such as laptops and hard drives that contain personal data, are encrypted so as to require not only passwords to be accessible but also secondary user confirmation (usually by requiring codes despatched to mobile phones to be inserted in the device to secure connection)
Papers containing confidential personal data must not be left on office desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
Passwords that are at least 8 characters long containing letters and numbers are used to access MAGIC MEDICAL computers, laptops and other electronic devices. Staff are reminded to change their passwords at regular intervals and that passwords must never be shared with anyone else
Staff, who store personal information on their personal devices are expected to follow the same security procedures as for MAGIC MEDICALowned equipment (see our ICT policies)
Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 5.5)
Where possible by anonymising or pseudonymising the data
5.5 Disclosure to Third Parties

Very rarely is personal data entrusted to third parties but whenever MAGIC MEDICALuses a third-party supplier or business partner to process personal data on its behalf, we will ensure that this processor will provide security measures to safeguard personal data that are appropriate to the associated risks. We will establish a

data sharing agreement with the supplier or contractor, to ensure the fair and lawful processing of any personal data we share.

MAGIC MEDICAL will contractually require the supplier or business partner to provide the same level of data protection as MAGIC MEDICALprovides. The supplier or business partner must only process personal data to carry out its contractual obligations towards MAGIC MEDICALor upon the instructions of MAGIC MEDICAL and not for any other purposes. When MAGIC MEDICALprocesses personal data jointly with an independent third party, MAGIC MEDICALwill explicitly specify its respective responsibilities of the third party in the relevant contract or any other legal binding document.
A list of such partners could be provided to Customers upon request provided there is a legitimate reason.

5.6 Rights of Access by Data Subjects

Individuals have a right to make a 'Subject Access Request' to gain access to personal information that MAGIC MEDICAL holds about them. This includes:

Confirmation that their personal data is being processed
Access to a copy of the data
The purposes of the data processing
The categories of personal data concerned
Whether the data has been, shared and, if so, with whom
How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
The source of the data, if not the individual
Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual
Subject access requests must be submitted in writing, either by letter or email to the DPO. They should include:

Name of individual
Correspondence address
Contact number and email address
Details of the information requested
A Data Subject Access Request Form will be sent to the individual.

5.8 Data Portability

Data Subjects have the right to receive, upon request, a copy of the data they provided to us in a structured format and to transmit those data to another controller.

5.9 Right to be Forgotten

Upon request, Data Subjects have the right to obtain from MAGIC MEDICAL the erasure of its personal data. When MAGIC MEDICALis acting as a Controller, we will take necessary actions (including technical measures) to inform the third-parties who use or process that data to comply with the request.

Fair Processing Guidelines
Personal data must only be processed when explicitly authorised by MAGIC MEDICAL.

MAGIC MEDICAL will decide whether to perform the Data Protection Impact Assessment for each data processing activity according to the Data Protection Impact Assessment Guidelines.

6.1 Notices to Data Subjects

At the time of collection or before collecting personal data for any kind of processing activities including but not limited to selling services, or marketing activities, we will inform data subjects of the following: the types of personal data collected, the purposes of the processing, processing methods, the data subjects' rights with respect to their personal data, the retention period, potential international data transfers, if data will be

shared with third parties and MAGIC MEDICAL's security measures to protect personal data. This information is provided through the General Data Protection (or Privacy) Notice.
Where personal data is being shared with a third party, we will ensure that Data Subjects have been notified of this through a General Data Protection Notice.

Where personal data is being transferred to a third country according to Cross Border Data Transfer Policy, the General Data Protection Notice will reflect this and clearly states to where, and to which entity personal data is being transferred.

Where sensitive personal data is being collected, we will make sure that the General Data Protection Notice explicitly states the purpose for which this sensitive personal data is being collected.

6.2 Obtaining Consents

Whenever personal data processing is based on the Data Subject's consent, or other lawful grounds, we will retain a record of such consent. We will provide Data Subjects with options to provide the consent and inform and ensure that their consent can be withdrawn at any time.

When requests to correct, amend or destroy personal data records, we will ensure that these requests are handled within a reasonable time frame. We will also record the requests and keep a log of these.

Personal data will only be processed for the purpose for which they were originally collected. In the event that MAGIC MEDICALwants to process collected personal data for another purpose , MAGIC MEDICAL will seek the consent of its Data Subjects in clear and concise writing . Any such request will include the original purpose for which data was collected , and also the new , or additional , purpose(s). The request will also include the reason for the change in purpose(s).

Now and in the future, we will ensure that collection methods are compliant with relevant law, good practices and industry standards.

Organisation and Responsibilities
The responsibility for ensuring appropriate personal data processing lies with everyone who works for or with MAGIC MEDICALand has access to personal data processed by MAGIC MEDICAL.

MAGIC MEDICAL administrative management board make decisions about, and approve MAGIC MEDICAL's general strategies on personal data protection.

Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
Performing regular checks and scans to ensure security hardware and software is functioning properly.
Improving all employees' awareness of user personal data protection.
Organising Personal data protection expertise and awareness training for employees working with personal data.
End-to-end employee personal data protection. It must ensure that employees' personal data is processed based on the employer's legitimate business purposes and necessity.
Passing on personal data protection responsibilities to suppliers and improving suppliers' awareness levels of personal data protection as well as flow down personal data requirements to any third party a supplier they are using.
Approving any data protection statements attached to communications such as emails and letters.
Addressing any data protection queries from general public, journalists or media outlets like newspapers.
Response to Personal Data Breach Incidents
When MAGIC MEDICAL learns of a suspected or actual personal data breach, an internal investigation needs to be conducted and appropriate remedial measures must be taken in a timely manner. Where there is any risk to the rights and freedoms of Data Subjects, MAGIC MEDICALmust notify the relevant data protection authorities without undue delay and, when possible, within 72 hours.

When the personal data breach or suspected data breach affects personal data that is being processed by MAGIC MEDICAL as a Data Controller, the following actions are performed:

MAGIC MEDICAL must establish whether the personal data breach should be reported to the Supervisory Authority.
In order to establish the risk to the rights and freedoms of the data subject affected, an internal Data Protection Impact Assessment must be performed on the processing activity affected by the data breach.
If the personal data breach is not likely to result in a risk to the rights and freedoms of the affected data subjects, no notification is required. However, the data breach should be recorded into the Data Breach Register.
The Supervisory Authority must be notified with undue delay but no later than in 72 hours, if the personal data breach is likely to result in a risk to the rights and freedoms of the data subjects affected by the personal data breach. Any possible reasons for delay beyond 72 hours must be communicated to the Supervisory Authority.
The notifications to the Supervisory Authority that will include the following:

A description of the nature of the breach
Categories of personal data affected
Approximate number of data subjects affected
Name and contact details of the Data Protection Officer
Consequences of the personal data breach
Measures taken to address the personal data breach
Any information relating to the data breach
Audit and Accountability
The administrative management board is responsible for auditing how well this Policy is implemented across MAGIC MEDICAL.

Any employee who violates this Policy will be subject to disciplinary action and the employee may also be subject to civil or criminal liabilities if his or her conduct violates laws or regulations.

Conflicts of Law
This Policy is intended to comply with the laws and regulations in the place of establishment and of the countries in which MAGIC MEDICALoperates. In the event of any conflict between this Policy and applicable laws and regulations, the latter shall prevail.

Managing records kept on the basis of this document
The administrative management board is responsible for the storage, updating and reviewing of all records maintained by MAGIC MEDICAL

The CTO of MAGIC MEDICAL has overall responsibility for this policy, and for reviewing the policy annually.