Privacy Policy

Last updated: 12/08/2025

1. Commitment and General Framework

AIM LIFE, Lda. (hereinafter AIM Cancer Center), as the entity responsible for processing personal data in the context of its clinical and business activities, is committed to ensuring the rigorous, effective, and secure protection of all personal data it collects and processes daily. This Privacy Policy clearly describes how we process your personal data and how you can exercise your rights as a data subject. AIM Cancer Center conducts all its activities in compliance with the General Data Protection Regulation (GDPR), Law No. 58/2019 of August 8 (national law implementing the GDPR), and other applicable sectoral legislation, particularly in the healthcare sector.

The security and privacy of personal data are paramount to AIM Cancer Center. We implement appropriate technical and organizational measures to protect data against loss, misuse, or unauthorized access, and we periodically review these measures to ensure continued compliance with best practices and legal requirements. AIM Cancer Center reserves the right to update or modify this Privacy Policy; any substantial changes will be communicated through appropriate channels. We recommend that you review this Policy regularly to stay informed about how we protect your privacy.

In addition to providing virtual cancer care, AIM Cancer Center also develops corporate health programs (AIM Corporate Health), training courses in various health areas, and participates in scientific research projects.

2. Personal Data and Personal Data Holders

What is personal data? Personal data is any information, of any nature and regardless of format, relating to an identified or identifiable natural person. Any person who can be identified directly or indirectly, in particular by reference to an identifier (e.g., a name, identification number, location data, online identifiers, or to one or more factors specific to their physical, physiological, genetic, mental, economic, cultural, or social identity), is considered identifiable.

Who are the holders of personal data that we process? As part of AIM Cancer Center's activities, personal data of a diverse range of data subjects is processed, including individuals and legal entities (the latter, to the extent that they contain data of representatives or employees). Without prejudice to other individuals who may be targeted, the main data subjects covered (not exhaustive) are:

- **Users/Clients** (patients of clinical services) and their employees or representatives (when the client is a legal entity);
- **Employees of partners or service providers** from the AIM Cancer Center;
- **Workers, job seekers or interns** from the AIM Cancer Center;
- **Event participants** organized or promoted by AIM Cancer Center;
- **Facility Visitors** of the AIM Cancer Center (including occasional visitors, speakers, vendors, etc.);
- **Also included are**: participants in corporate health programs and corporate well-being initiatives; trainees or enrolled in training courses promoted by AIM; participants in scientific research projects conducted or co-organized by AIM.

3. What Personal Data We Collect and How

AIM Cancer Center collects only adequate, relevant personal data, limited to what is strictly necessary for the specific purposes of the processing (in accordance with the GDPR data minimization principle). Collection may occur through various means and at various times, including:

i) **orally** (e.g. by telephone or video call),

ii) **in writing** (through forms, registration forms, contracts or other physical documents), or

iii) **digitally** (through the institutional website and other AIM Cancer Center online platforms).

Collection in person at our facilities only occurs in exceptional cases, as AIM Cancer Center mostly provides services remotely.

As a general rule, we collect your data directly, although in some situations we may obtain data through duly authorized third parties or in the context of partnerships (e.g. receiving analysis results from external laboratories, professional references from candidates, etc.).

Categories of personal data processed: Depending on the purpose in question, we may collect and process the following categories of personal data:

- **Identification data**– such as full name, marital status, place of birth, date of birth, identification document number (Citizen Card or equivalent) and SNS user number, where applicable;
- **Contact details**– such as address, email address, telephone/mobile number;
- **Academic and professional data**– such as academic qualifications, academic history, current professional situation or position/function performed (only for employees, collaborators of partner entities or candidates for job/internship vacancies);
- **Financial and billing data**– such as Tax Identification Number (NIF), IBAN, health insurance or health subsystem data (if applicable to payment for care), billing and transaction information;
- **System usage data and electronic location**– such as IP addresses, access log data to computer systems or the AIM Cancer Center Wi-Fi network (when provided), records of use of devices or applications made available by AIM Cancer Center, etc.;
- **Images and sound**– namely, image recordings (and sound, if applicable) obtained in the context of training, events or video conferences promoted by AIM Cancer Center (with prior notice) and images captured by video surveillance systems (CCTV) installed in our facilities, as described below in Section 10 of this Policy;
- **Health data (sensitive personal data)**– information relating to your physical or mental health status, medical history, test results, diagnoses, treatments, and other

data included in your patient's clinical file, as well as other data belonging to special categories under the GDPR (such as genetic or biometric data for identification purposes, if and when applicable). Due to their highly sensitive nature, this data is processed exclusively in the context of providing healthcare or managing the clinical file, with special confidentiality and security safeguards (as detailed later in this Policy). Please note that AIM Cancer Center does not, as a rule, collect special categories of data unrelated to the clinical context (such as religious, philosophical, or political beliefs, data on sexual life, ethnic origin, or trade union membership), except when strictly necessary and in the context of providing healthcare, and always subject to appropriate legal exceptions.

All information collected in connection with the use of the website (including, for example, data submitted through contact forms or pre-booking appointments) will be used exclusively for the purposes communicated at the time of collection (e.g., responding to your contact, processing your registration or scheduling the requested appointment) and to improve the user's browsing experience on the website. For information on the use of cookies or similar technologies on our website and application, please see our Cookie Policy available online.

4. Grounds for the Lawfulness of Processing

Why (and on what legal basis) do we process your personal data? All personal data processing carried out by AIM Cancer Center has a valid lawful basis under Article 6 of the GDPR (or Article 9 in the case of special categories of data, as explained below). Specifically, depending on the specific purpose, the processing will be based on one of the following lawful grounds:

- **Data subject consent:** when you have given us free, explicit, informed, and specific consent to process your data for a specific purpose. For example, we will request your prior consent to use your email address to send newsletters, or to process personal data for marketing purposes or to promote events not directly related to the services you have contracted. You may withdraw your consent at any time, as explained below in your rights.
- **Execution of contract or pre-contractual due diligence:** when data processing is necessary for the conclusion, performance, and management of a contract to

which the data subject is a party, or for taking steps at the data subject's request prior to entering into a contract. For example, we will use personal data necessary to draw up and execute healthcare (or other service) contracts with our users and clients, to execute employment contracts with our employees, or service provision contracts with suppliers and partners. This includes essential pre-contractual data processing (e.g., processing job/internship applications, budgeting for healthcare services prior to hiring).

- **Compliance with legal obligations:** When processing is necessary to comply with legal obligations to which AIM Cancer Center is subject. In these situations, your data will be processed to the extent necessary to comply with applicable national or European Union laws and regulations. For example, we may need to communicate personal data to public health entities or regulatory authorities (such as the Central Administration of the Health System (ACSS), the Health Regulatory Entity (ERS), or the Directorate-General for Health (DGS), tax and fiscal authorities, social security, courts, or police authorities, in the cases provided for by law. Likewise, in the employment context, we process data to comply with obligations arising from the Labor Code and tax and social security legislation (e.g., mandatory communications to Social Security, the Labor Compensation Fund, the Authority for Working Conditions, among others).

- **Legitimate interest of the person responsible or third parties:** when processing is necessary for the purposes of legitimate interests pursued by AIM Cancer Center or third parties, provided that the rights, freedoms, and guarantees of the data subject do not prevail. This basis may be applied, for example, to ensure the physical security of facilities, property, and people (video surveillance and access control, due to our legitimate interest in protecting all stakeholders), to prevent fraud and safeguard computer systems (our interest in protecting our business from unauthorized access or cyberattacks), or even for the exercise or defense of rights in legal proceedings (our legitimate interest in defending ourselves or asserting rights in litigation) when we are not required by law to retain such data. In any case where we rely on legitimate interest, we will conduct a prior assessment to confirm that our interest does not excessively conflict with the rights of the data subjects.

- ***Processing of special categories of data (sensitive data)*:** With regard to health data or other sensitive data that we may process, it is important to note that the basis for lawfulness will not, as a rule, be the data subject's consent, but rather the legal exceptions provided for in Article 9(2) of the GDPR. Specifically, AIM Cancer Center processes users' health data because it is necessary for the purposes of preventive medicine, diagnosis, provision of health care or treatment, or management of health systems, under Article 9(2)(h) of the GDPR, and in compliance with applicable national legislation that imposes the duty of professional secrecy on health professionals. Therefore, health data is processed exclusively by or under the direction of professionals subject to a duty of confidentiality (doctors, nurses, diagnostic technicians, etc.), and the data subject's express consent is not required for these processes in the context of the provision of health care, as they are based on a special legal provision and professional obligation. This clarification aligns with the GDPR and Law 58/2019 (Art. 29) and aims to ensure that the data subject understands that, for legal and quality of care reasons, they cannot refuse the processing of their clinical data essential to care by invoking lack of consent, except in strictly applicable situations (for example, processing outside the clinical scope, such as certain research projects or marketing actions, which will only occur with consent, if they are to process health data).

5. Purposes of Personal Data Processing

The personal data collected by AIM Cancer Center is intended for specific, explicit, and legitimate purposes, communicated at the time of collection or in this Policy. We will not process your data in a manner incompatible with these purposes. Below, we present the main purposes for which data is processed by AIM Cancer Center, indicating the respective legal basis in each case:

- **Healthcare provision and clinical management:** includes scheduling appointments, performing tests, diagnosis, therapy, and clinical monitoring in the context of the relationship with the user. Legal basis: execution of the health service provision contract with the data subject (necessary to provide the requested service) and compliance with legal obligations in the health area; in the

case of health data involved, the legal exception of Art. 9(2)(h) of the GDPR also applies, as described above, and consent is not required.

- **Drafting, negotiation and execution of commercial or employment contracts:** management of contracts with customers, service providers, suppliers, employees and other parties, including payment processing, invoicing, human resources management, etc. Legal basis: necessity for the performance of a contract or pre-contractual diligence (Art. 6(1)(b) GDPR) and, where applicable, compliance with legal obligations (e.g. employment and tax obligations).
- **Organization and management of events and training activities:** Registration and participation of interested parties in events, training sessions, workshops, or initiatives promoted by AIM Cancer Center, including attendance management, issuing of certificates, and use of images when authorized. Legal basis: depending on the case, consent of the data subject (e.g., for the use of images or sending of invitations) or performance of a contract (if the event is part of a requested service).
- **Management and execution of corporate health programs (within the scope of AIM Corporate Health)**: including communication with participants and contracting companies.
- **Implementation and monitoring of scientific research projects**: including data collection and analysis for study purposes, always based on informed consent and/or other applicable legal bases.
- **Dissemination of newsletters and marketing communications:** sending informative newsletters and communications about AIM Cancer Center services, campaigns, or events that may be of interest to the data subject. Legal basis: explicit consent of the data subject for this purpose (Art. 6(1)(a) GDPR), obtained, for example, when voluntarily subscribing to the newsletter. The data subject may withdraw consent at any time, in which case they will no longer receive these communications.
- **Physical security of people and facilities:** monitoring and controlling access to AIM Cancer Center facilities, CCTV video surveillance in designated areas, recording entries and exits, and implementing security measures to protect

employees and other visitors, as well as property and infrastructure. Legal basis: legitimate interest of the controller in preventing incidents, protecting people and property, and deterring illegal practices (Art. 6(1)(f) GDPR); compliance with legal obligations regarding private security (where applicable, e.g., Law 34/2013) and, where applicable, protecting vital interests (Art. 6(1)(d) in emergencies). (See Section 10 below for specific details on video surveillance.)

- **Computer systems management and information security:** maintenance and monitoring of our information technology systems, including user account management, backups, prevention of fraud, intrusion or cyberattacks, and ensuring service continuity. Legal basis: legitimate interest in protecting the network and systems (Art. 6(1)(f)) and compliance with legal obligations regarding data security (e.g., duties imposed by the GDPR on security, in particular in Art. 32).

- **Exercising rights in legal proceedings and responding to legal requests:** use of personal data as necessary to establish, exercise or defend legal or administrative claims, either by AIM Cancer Center or in the context of cooperation with authorities (e.g., responding to court orders, warrants or requests from the CNPD). Legal basis: legitimate interest in protecting our rights (Art. 6(1)(f)) and/or compliance with a legal obligation (Art. 6(1)(c)), as the case may be. In the case of special categories of data strictly necessary for this purpose (e.g., health data to demonstrate due diligence in court), the basis will also be covered by the exception in Art. 9(2)(f) of the GDPR (necessary for the establishment, exercise or defense of a right in legal proceedings).

- **Compliance with specific legal obligations:** Data processing to comply with sectoral obligations, such as reporting obligations to health authorities, recording and maintaining hospital clinical records, complying with tax and accounting obligations, or collaborating with regulatory authorities. Legal basis: compliance with legal obligations (Art. 6(1)(c)) – see examples in the grounds section above (communications to ACSS, ERS, Tax Authority, etc.).

- **Other auxiliary or complementary purposes:** We may process data to continuously improve our services (e.g., anonymized or minimally invasive satisfaction surveys), for internal audit and compliance activities, or as part of

corporate transactions (e.g., data transfer in the event of a merger or spin-off, always in compliance with the applicable legal bases). In these situations, we will assess the applicable legal basis on a case-by-case basis (legitimate interest, legal obligation, or consent, depending on the nature of the processing) and inform data subjects as required.

In any case, AIM Cancer Center guarantees that it does not process data for purposes incompatible with those described herein, nor does it make exclusively automated decisions that produce significant effects on data subjects without the appropriate legal basis and prior information (note: currently, AIM Cancer Center does not perform profiling or significant automated decisions on users or clients, given that clinical decisions always involve qualified human intervention; if this scenario changes in the future, data subjects will be informed accordingly).

6. Personal Data Retention Period

AIM Cancer Center processes and stores your personal data only for the period strictly necessary to achieve the specific purposes of the processing, in compliance with the legally required or recommended timeframes. This means that, once the purpose for which the data was collected has been achieved, we will delete or anonymize it, unless there is a legal obligation to retain it for an additional period or another legitimate basis for retention.

General conservation rules: In many cases, the duration of processing will coincide with the duration of the contractual relationship or the service provided. Therefore, if we have a contract with you (e.g., a healthcare contract or an employment contract), your essential personal data will be retained for the duration of that contractual relationship. Subsequently, some data may continue to be retained for as long as necessary to fulfill post-contractual or legal obligations (e.g., warranty periods, legal prescriptions, or pending legal proceedings). We also have legal obligations that impose minimum retention periods for certain types of data: for example, personal data in billing documents must be kept for 10 years to comply with tax and accounting obligations (in accordance with Portuguese tax law). We may also retain certain data while there are pending legal proceedings, claims, or debts relating to the data subjects, for the period necessary until these situations are finally resolved (thus ensuring their timely deletion). After the

applicable periods have expired, we will securely delete or irreversibly anonymize the data.

Preservation of video surveillance images: Images collected by our CCTV systems on our premises are retained for a maximum period of 30 (thirty) days from the date of capture. This period complies with national private security legislation and CNPD guidelines, which generally limit the retention of video surveillance recordings to one month (unless an incident occurs that justifies retention for a longer period for evidentiary purposes). Therefore, after the 30-day period, the recordings are automatically deleted, unless a significant incident occurred during the period in question (e.g., an accident, theft, or other unlawful act) that justifies the retention of the specific recording for a longer period, limited to the need for delivery to the competent authorities or to support legal proceedings. In these exceptional cases, the images in question will be retained only for the additional time necessary and will be deleted as soon as the purpose of the extraordinary retention expires.

In general, we maintain internal documentation defining the retention periods applicable to each category of data under our care, taking into account legislation and the recommendations of the supervisory authority (CNPD). We strive to ensure that, once the purpose has been fulfilled and the necessary or legally required period has elapsed, personal data is effectively deleted or anonymized. If, for technical or operational reasons, we are unable to immediately delete/anonymize certain backup data, we will isolate and protect it until deletion is feasible. If you have questions about the specific retention periods applicable to your personal data, please contact us for further clarification.

7. Rights of Personal Data Holders

As the data subject, you have a set of rights regarding the data you have provided to us or that we have collected about you. AIM Cancer Center values these rights and provides you with the means to exercise them, in accordance with applicable legislation. In summary, you have the right to:

- **Right of Access:** obtain confirmation as to which personal data are or are not being processed by AIM Cancer Center and, when they are, access them and the information associated with the processing (purposes, data categories, recipients

to whom they were or will be disclosed, expected retention periods, existence of rights to rectification/erasure/opposition, source of the data, and possibly the existence of automated decisions). Upon request, we will provide you with a copy of the personal data being processed, in a commonly used electronic format or another suitable format.

- **Right of Rectification:** Request the correction or update of your personal data if it is incorrect, outdated, or incomplete. It is important that the data we process about you is accurate and current; therefore, please inform us whenever there is a need to change, for example, your contact address or other relevant details.
- **Right to Erasure of Data**(or "right to be forgotten"): request the deletion of your personal data, where legally permitted. This right can be exercised, for example, when the data is no longer necessary for the purpose for which it was collected, when you withdraw consent (in cases where processing is based solely on consent), or when you object to processing based on legitimate interest and there are no overriding interests to justify it. It is important to note, however, that this right is not absolute – it may not be possible to immediately delete certain data if a legitimate basis for retaining it remains (such as compliance with a legal retention obligation or the need for preservation to exercise rights in legal proceedings). In such cases, we will inform the data subject of the reasons why deletion is not possible and will ensure that the data remains blocked for other purposes.
- **Right to Limitation of Processing:** Obtain restriction of the processing of your personal data, temporarily suspending it, in situations provided for in the GDPR – for example, while the accuracy of the data (after a request for rectification) or the legitimacy of the processing (after objection) is being discussed, or even when AIM Cancer Center no longer needs the data, but the data subject requests that we keep it for the purposes of declaring, exercising or defending a right in a legal proceeding. When processing is limited, the data (beyond mere storage) may only be processed with the data subject's consent or for very limited purposes (as referred to in Article 18 of the GDPR).
- **Right to Portability:** receive the personal data you provided to us in a structured, commonly used, and machine-readable format and transmit that data to another

data controller, or request, where technically feasible, that AIM Cancer Center transfer it directly to another entity designated by you. This right applies only when the processing is based on consent or the performance of a contract and is carried out by automated means.

- **Right of Objection:** Object, for reasons related to your particular situation, to the processing of your personal data based on the legitimate interest of the controller. In this situation, we will evaluate your request and cease the processing in question, unless we have compelling legitimate grounds to continue or if the data is necessary for the establishment, exercise, or defense of a legal claim. Additionally, you always have the right to object, at any time and without justification, to the processing of your data for direct marketing purposes, including profiling related to such marketing. If you exercise this right to object in the context of marketing, we will immediately cease using your data for that purpose.
- **Right to Withdraw Consent:** In cases where data processing is based solely on your consent, you have the right to withdraw that consent at any time. Withdrawing consent does not compromise the lawfulness of any processing previously carried out based on your consent. If you withdraw consent for a specific purpose, we will no longer process your data for that specific purpose (e.g., to stop sending newsletters), but we may continue to process the same data for other purposes if we have another legal basis for doing so.

In addition, you also have the right not to be subject to automated individual decisions (including profiling) that produce legal effects or significantly affect you, except in the cases provided for by law. Note: AIM Cancer Center does not use exclusively automated decision-making processes on user data that meet the relevant criteria of Article 22 of the GDPR, so this right, while recognized, is somewhat theoretical in our context (all clinical and service decisions involve qualified human intervention). If we implement any such automated decision-making system, we will inform data subjects and ensure compliance with the additional requirements provided for by law.

How can you exercise your rights? The exercise of these rights is free of charge (except in cases of manifestly unfounded or excessive requests, in which case we may charge a reasonable fee or refuse, pursuant to Art. 12(5) of the GDPR) and can be made at any

time. To exercise any of the above rights, you must submit a clear and written request, accompanied by information that allows us to confirm your identity (e.g., full name and, if necessary, a copy of an identification document, solely to verify that you are the data subject). This request can be sent by:

- **E-mail:** via email address **geral@aim.clinic**;
- **Written communication:** via letter sent to the postal address of AIM Cancer Center (addressed to the Data Protection Officer) or delivered in person at our facilities, upon receipt;
- **Online form:** If AIM Cancer Center provides a dedicated data protection form on its website, you can use it (currently, the main channels are those indicated above).

We will do our best to respond to your request promptly and within a maximum period of 1 month from receipt, as provided for in the GDPR. In cases of particularly complex or multiple requests, this period may be extended up to 2 months, but in this case, we will inform you of this need within the first month. Our response to your requests will be in writing (usually by email, unless you request otherwise) and will include the information required by law. If, for any reason, we cannot comply with your request (for example, due to a conflict with applicable legal obligations), we will provide a clear justification.

Finally, we remind you that you also have the right to file a complaint with the competent supervisory authority if you believe that the processing of your data by AIM Cancer Center violates the GDPR or other data protection regulations. In Portugal, the supervisory authority is the CNPD – National Data Protection Commission (website: www.cnpd.pt). We encourage you, however, to contact us directly (yourself or through our DPO) before making any complaint so that we can clarify or resolve your issue promptly – we are committed to protecting your data and addressing any concerns you may raise in good faith.

8. Communication of Data to Third Parties and Subcontractors

Who do we share your personal data with? In the course of our business, and strictly for the defined purposes, your personal data may be shared with third parties when necessary or mandatory. We ensure that this sharing occurs within the limits of the law and this Policy, and that we only provide recipients with the information essential for

each legitimate purpose. The main categories of recipients or third parties to whom we may disclose data (as applicable in each case) are:

- **Public authorities and official bodies:** including government or regulatory entities in the health sector (e.g. Ministry of Health, DGS, ACSS, ERS), judicial or police authorities, jurisdictional bodies or independent administrative authorities (such as the CNPD, Tax Authority, Social Security, ACT), when such communication is required by law or necessary to comply with legal/regulatory obligations.
- **Other healthcare providers or healthcare entities:** In cases where it is necessary to involve clinical analysis laboratories, partner clinics or hospitals, referred physicians, or other external healthcare professionals in the provision of patient care, health data will be shared with the patient's knowledge and/or request (e.g., referral to another specialist, request for an additional external examination) and under the obligation of medical confidentiality, ensuring that the recipient is also bound by confidentiality. Similarly, if the patient is covered by a health insurance plan or subsystem and requests activation of this plan, we may communicate billing data and strictly necessary clinical information to the insurer or paying entity for the purposes of payment/reimbursement for services provided.
- **Financial institutions and insurance companies:** Banks, payment processors, health or occupational accident insurance companies, pension funds, and other similar entities, when the processing so requires. For example, to bill for clinical services, we may send payment references to banks or payment processors; in the event of an employee's work-related accident, we will need to notify the respective insurance company with the claim details; if the user activates health insurance, we may confirm certain processing details to the insurer to validate coverage. These communications will always be made on an appropriate legal basis (compliance with an insurance contract, legal obligation, or legitimate interest, depending on the context).
- **External consultants and research sponsors:** in specific circumstances, we may have to share some personal data with legal consultants, auditors, experts or other contracted consultants who are bound by a duty of confidentiality (for example, in the context of quality audits, compliance assessments or legal defense), or even – with the prior consent of the data subject, when required – with entities

sponsoring clinical studies or research projects in which the user participates (in these cases, whenever possible, the data will be pseudonymized or anonymized).

- **Service providers (subcontractors):** Partners and external companies that provide services to AIM Cancer Center and may need to process personal data on AIM Cancer Center's behalf (thus acting as subcontractors, pursuant to Article 28 of the GDPR). These include, for example: information technology services (system maintenance, database hosting, cloud service provider), document archiving and scanning services, certified document destruction companies, IT and telecommunications support services, private security companies (in the case of security guards who may have access to CCTV images in real time), mail delivery or logistics services, among others necessary for our business. In these situations, AIM Cancer Center enters into written contracts with such entities, imposing on them data protection obligations equivalent to those we observe, including confidentiality duties, appropriate technical and organizational measures for information security, and the guarantee that they act only in accordance with our explicit instructions. In short, subcontractors cannot use the data for their own purposes and are legally and contractually bound to protect the personal data we entrust to them. AIM Cancer Center carefully selects these partners and only uses entities that offer sufficient guarantees of compliance with data protection regulations.

When sharing data with third parties, AIM Cancer Center adheres to the principle of the minimum necessary, transmitting only adequate, relevant data, limited to what is strictly necessary to fulfill the purpose in question. Whenever required by law, we will request your prior consent or provide you with the opportunity to object to a particular transfer.

9. International Data Transfers

As a rule, AIM Cancer Center processes and stores personal data on servers located within the European Economic Area (EEA) or in countries that ensure a level of protection equivalent to that of the EU. However, in certain specific cases, it may be necessary to transfer some personal data outside the EEA – for example, if we use cloud services or digital platforms whose servers are located in third countries, or if it is necessary to send information to a healthcare institution in a third country at the data subject's request.

In these international transfer situations, AIM Cancer Center strictly complies with applicable legal provisions (Articles 44 to 49 of the GDPR), ensuring that the transfer only occurs to countries considered to be at an adequate level by the European Commission or through the implementation of approved appropriate safeguards (such as European Commission Standard Contractual Clauses, binding rules applicable to the processor, or a specific international agreement). We will provide additional relevant information to the data subject whenever necessary and will suspend any transfer of data outside the EU if the required security and legality conditions are not met.

In short, if your data needs to be transferred outside of Portugal/the EU, we will ensure it remains protected according to European standards and will keep you informed as required by law. For more details on international data transfers (or to obtain a copy of the safeguards implemented), please contact us through the channels provided.

10. Video Surveillance and Physical Security on the Premises

AIM Cancer Center uses video surveillance (CCTV) systems throughout its facilities, in strategic public access and circulation areas (e.g., main entrances, reception, restricted-access corridors, parking lots), to ensure the safety of people and property, prevent illegal incidents, and deter crime within the monitored perimeter. The presence of video surveillance cameras is clearly marked in monitored areas, containing the legally required information (camera pictogram and a brief description of the purpose and the responsible entity). This measure ensures that all employees and other visitors are aware of any footage being captured, in compliance with Law No. 34/2013 (private security regime) and the CNPD's guidelines on video surveillance.

Purpose and legal basis: The sole purpose of video surveillance is security—protecting employees, visitors, and facilities against theft, vandalism, violence, or other security emergencies. We do not use the footage for any other purpose (e.g., monitoring employee performance or monitoring visitors unrelated to security). The primary legal basis for this processing is AIM Cancer Center's legitimate interest in ensuring security (Art. 6(1)(f) GDPR), combined with the legal authorization granted by private security legislation that allows the installation of CCTV in private establishments to protect people and property. In certain situations, processing (viewing and delivering recordings) may also be

necessary to comply with a legal obligation (e.g., responding to a request from law enforcement or judicial authorities in the context of a criminal investigation).

Location of cameras: For security reasons, we do not publicly disclose the exact location and number of installed cameras. However, we can inform you that the cameras only cover common areas and public or security access areas within AIM Cancer Center facilities. There are no cameras in private areas such as private offices, restrooms, private waiting rooms, or other locations where there may be a high expectation of privacy. The cameras are positioned so as not to capture unnecessary images of exterior public roads (except when strictly necessary to cover entrances) or interiors of third-party spaces.

Access to images: The images recorded by the CCTV system are stored securely and with restricted access. Only individuals authorized by AIM Cancer Center, within the scope of their security or administrative functions (e.g., the facility security officer or administrative management), or possibly the subcontracted private security company (if monitoring is outsourced), may access the recordings, and always under strict confidentiality obligations. Access occurs only when necessary (e.g., to verify a reported security incident). All these individuals are subject to a legal and contractual duty of confidentiality regarding the images. In the event of a significant incident, the relevant images may be transmitted to the appropriate authorities (law enforcement or courts), upon legal request, for investigation purposes. The recordings are never made publicly available or used internally for purposes other than security.

Storage periods: As mentioned in Section 6, video surveillance recordings are retained for a maximum period of 30 days from their capture, after which they are automatically deleted (overwritten), unless an incident is detected within that period that justifies retention for a longer period. If, for example, a theft or other relevant event captured by the cameras is reported, the footage required to prove that event may be isolated and retained for an additional period, strictly until the conclusion of the investigation or associated legal proceedings, after which it will be immediately deleted. This procedure is aligned with applicable law and industry best practices, ensuring that we do not retain video surveillance data longer than necessary.

Rights of holders regarding images: Any data subject has the right to contact us to request access to CCTV footage in which they may appear (right of access, provided this

does not affect the rights of third parties), as well as to exercise the other rights mentioned in Section 7 (e.g., objection or restriction, if applicable). Please note that, for technical and security reasons, requests for access to video surveillance recordings must indicate the date, time, and approximate location where the data subject was under surveillance, so that we can identify the existence of images depicting them. We must also ensure that a data subject's access does not compromise the privacy of third parties present in the footage – if necessary, we may take measures to obscure third parties or invite the data subject to view the footage in person at our facilities, in a controlled environment. Early deletion of recordings may also be requested, but will only be carried out if this does not conflict with our legitimate security interests or legal obligations (e.g., if the footage is no longer needed because the data subject has proven that the capture was unlawful). All requests will be assessed on a case-by-case basis, in accordance with the law, and should be addressed to our Data Protection Officer, using the contact details below.

Notice: Given that AIM Cancer Center is a virtual clinic, providing oncology care primarily remotely and digitally, the physical presence of a patient at AIM Life facilities is exceptional and rarely occurs. Therefore, it is not expected that, within the scope of this section, the data processed will be subject to the patient's data.

11. Technical and Organizational Security Measures

AIM Cancer Center adopts appropriate technical and organizational security measures to protect personal data against destruction, loss, alteration, unauthorized disclosure, or access, as well as against any form of accidental or unlawful processing. We are aware of the special sensitivity of much of the data we process (particularly health data) and, therefore, have implemented enhanced safeguards in this regard. In general, we highlight the following security measures and practices in place:

- **Access control and restriction by profile:** Personal data is only accessible to AIM Cancer Center employees or subcontractors who truly require such data to perform their duties (need-to-know principle). In particular, patient clinical and health data is only accessible to healthcare professionals directly involved in care (doctors, nurses, technicians) and supervised support staff (e.g., administrative staff who enter data into processes or IT technicians who maintain systems), all of whom are bound by legal and contractual obligations of secrecy and

confidentiality. We employ strong authentication systems (unique credentials, robust and periodically renewed passwords, access cards/keys, etc.) to ensure that only authorized users access databases or restricted physical areas.

- **Training and awareness:** All AIM Cancer Center employees, especially those who handle personal data (especially sensitive data), receive regular data protection and information security training. They are also required to sign confidentiality agreements upon joining their positions and strictly adhere to internal data protection policies. The privacy culture is reinforced through internal communications, information sessions led by the DPO, and updates whenever necessary, ensuring that the duty of professional secrecy and the protection of personal data are values instilled throughout the organization.
- **Technological protections:** We use recognized, reliable technical security solutions, such as firewalls for network perimeter protection, intrusion detection and prevention systems (IDS/IPS), up-to-date antivirus and antimalware, encryption mechanisms for sensitive data (at rest and in transit, where applicable), and regular backups of critical systems (stored securely, with controlled access). Our servers and infrastructure are maintained in data centers with robust physical security controls and redundancy, mitigating the risk of failures or unauthorized access.
- **Pseudonymization and minimization:** Whenever possible and appropriate, we use pseudonymization of personal data, especially in secondary processing contexts (e.g., clinical research or internal statistics), so that data subjects are not directly identifiable without the use of additional, separate information. We maintain minimization policies that determine that each department or system only collects the data necessary for the intended purpose (avoiding excessive collection) and that such data is stored for the shortest time necessary (as per Section 6).
- **Activity and audit log:** We maintain log records of access and operations performed on systems that process personal data, particularly clinical record management systems, to enable monitoring and auditing of unauthorized access or unauthorized data searches. We conduct periodic internal audits (and, when necessary, independent external audits) to assess compliance with policies and legal requirements, covering information security, among others.

- **Incident Response Plans:** In the event of a security incident affecting personal data, all employees must immediately report the incident to the DPO and senior management, to allow for the rapid containment and correction of the situation, the assessment of the risks to data subjects and, where applicable, notification to the CNPD and the affected data subjects themselves, in accordance with Articles 33 and 34 of the GDPR.
- **Continuous assessment and review:** The security measures implemented are periodically reassessed and updated based on technological developments, newly identified threats, or changes in the risk landscape. Additionally, for new projects, products, or services involving personal data, we apply the privacy by design principle and conduct Data Protection Impact Assessments whenever the proposed processing is likely to pose a high risk to the rights of data subjects (Art. 35 GDPR).

With these measures, AIM Cancer Center aims to fully comply with the provisions of Article 32 of the GDPR and other relevant national regulations, ensuring a level of security appropriate to the risk. Despite all our efforts, it is important to note that no security system is absolutely infallible; nevertheless, we are committed to implementing all reasonable efforts to protect personal data and to acting promptly in the event of a data breach or suspected data breach, mitigating any adverse effects.

12. Data Protection Officer (DPO) and Contacts

National Data Protection Authority: We reiterate that, if you deem it necessary, you have the right to file a complaint with **National Data Protection Commission(CNPD)**, the regulatory authority in Portugal for these matters. AIM Cancer Center hopes, however, to be able to satisfactorily address all your concerns without the need for the involvement of the CNPD, voluntarily and in good faith adhering to best data protection practices.

AIM Cancer Center appreciates the trust you have placed in us and assures us that the personal data entrusted to us will be treated with the utmost responsibility, confidentiality, and integrity. This Privacy Policy reflects our ongoing commitment to respecting your

privacy and scrupulously complying with applicable data protection legislation. If you have any questions about any of the contents of this Policy or how to exercise your rights, please do not hesitate to contact our DPO or our services. We are available to assist and clarify any questions you may have, because protecting your data is as important to us as providing excellent care.