PERSONAL DATA PROTECTION POLICY

Index

1. Purpose and Scope

AIM LIFE, Lda. (AIM Cancer Center) values the privacy and protection of personal data, having practices and instruments in the area of security and data protection, as well as ensuring compliance with the provisions of Regulation (EU) 2016/679, of the European Parliament and of the Council, of April 27, 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data - General Data Protection Regulation (GDPR) - and in Law No. 58/2019, of August 8, which ensures the implementation of the GDPR in the Portuguese legal system.

AIM Cancer Center applies appropriate technical and organizational security measures to ensure that the processing of personal data is lawful, fair, transparent and limited to authorized purposes, ensuring a level of personal data security appropriate to the risk, in compliance with the GDPR.

In this sense, this procedures manual and its annexes define the general principles and rules to be applied by AIM Cancer Center as the controller of the Personal Data collected by it.

The AIM Cancer Center personal data protection policy that we now intend to implement is associated with a set of procedures and aims to clarify and regulate how AIM Cancer Center, its employees and collaborators must comply with the aforementioned legal provisions.

Those responsible for each area must ensure that their respective activity and the processes inherent to it comply with the AIM Cancer Center's personal data protection policy and provide training for their employees, who must follow and comply with all procedures established in this area as an obligation inseparable from their respective duties.

Compliance with the personal data protection policy is mandatory for all AIM Cancer Center employees, management, and anyone who wishes to collaborate with AIM Cancer Center.

This Policy is part of a broader set of AIM Cancer Center privacy and data protection documents. In particular, it should be read in conjunction with the Privacy Policy, Cookie Policy, Terms and Conditions, current data processing outsourcing agreements, and AIM Cancer Center's Data Processing Responsibility, Joint Liability, and Outsourcing Policy.

In case of doubt, the necessary clarification should be requested from AIM Cancer Center.

2. Concepts and Principles

2.2. **Main Concepts**

a) *Personal Data:* Information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier. Examples of personal data:

- Name;
- Address or email address;
- CV;
- Social security number or NIF;
- Vehicle registration;
- Location data;
- CCTV recordings (video surveillance cameras);
- Pay slips;
- Business cards;

b) *Special data:* personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as the processing of genetic data, biometric data to uniquely identify a person, data concerning health or data concerning a person's sex life or sexual orientation.

c) *Processing of Personal Data:* an operation or set of operations performed on personal data, by automated or non-automated means, such as collection, recording, organization, structuring, storage, alteration, recovery, consultation, use, transmission, interconnection, limitation, erasure or destruction.

d) *Responsible for processing:* the entity (public or private) that, individually or jointly with others, determines the purposes and means of processing personal data. Within the context of AIM Cancer Center's activities, it generally

assumes the role of Data Controller for the personal data it collects, but may also act as Processor or Joint Controller in certain situations.

e) *Subcontractor:* entity (public or private) that processes personal data on behalf of the person responsible for processing them;
f) *Third:* entity (public or private) that is not the data subject, the controller or the processor, but which is authorized to process personal data;
g) *Responsible area:* corresponds to the area of AIM Cancer Center responsible for each operation involving the processing of personal data, i.e., the area that defines the purposes and means of such processing;
h) *Third area:* corresponds to the area of AIM Cancer Center that, although not the responsible area, needs to access personal data processed by other areas of AIM Cancer Center;
i) *Data Breach:* breach of personal data originating from a security failure (physical or logical) that compromises the confidentiality, integrity and availability of personal data (i.e., which may lead to the destruction, loss, alteration, access or unauthorized disclosure of personal data);
j) *Data Protection Impact Assessment (DPIA):* Prior procedure to be carried out by AIM Cancer Center whenever data processing, in particular using new technologies and taking into account its nature, scope, context and purposes, is likely to entail a high risk to the rights and freedoms of natural persons.
k) *Data Protection Officer (DPO):* designation (and functions) published through a Service Order and communicated to the national data protection supervisory authority.

2.2 Principles governing the processing of personal data

When collecting and processing personal data entrusted to them, AIM Cancer Center and its employees and collaborators must base their conduct on the following principles:

- *Principle of Transparency, Legality, Loyalty:* the processing of personal data must be lawful, fair and transparent;

- *Minimization Principle:* the processing of personal data must be adequate, relevant and limited to what is necessary to fulfill the purpose(s);
- *Principle of Limitation of Treatment:* personal data must be processed for specific, explicit and legitimate purposes, and the processing must be limited to the purpose(s) for which the data are collected; on the other hand, the data must be kept until the end of the purpose for which they were collected or, if longer, to comply with legal deadlines or during the pendency of legal proceedings;
- *Principle of Accuracy:* only accurate and up-to-date data should be processed;
- *Data Protection Principle by Default:* By default, only the personal data that is necessary for each purpose should be processed (regarding the amount of personal data collected, the extent of its processing, its retention period and its accessibility).
- *Principle of Data Protection by Design:* the duty to apply appropriate technical and organizational measures, both when defining the means of processing and at the time of processing, to guarantee these principles and the exercise of the rights of data subjects, as well as to guarantee the confidentiality, integrity, and availability of the data. Records associated with the various processing operations must also be kept for monitoring purposes;

3 Legality conditions, forms of collection and types of data and data subjects

3.1 Fundamentals inherent to data processing by AIM Cancer Center

All data collected and processed by AIM Cancer Center is based on one of the following legal conditions:

- *Consent:* When collection and processing are preceded by the express, specific, free, and informed consent of the data subject, provided in writing or via the web. Consent is collected, for example, when the data subject provides a set of personal data for the purposes of a proposal or quote, or to subscribe to direct marketing campaigns. Whenever consent is the condition for lawfulness, it must expressly state the purpose of the processing and refer to the AIM Cancer Center Privacy Policy;
- *Execution of contract or pre-contractual due diligence:* when the processing is necessary for the performance of a contract to which AIM Cancer Center and

data subjects are parties or for pre-contractual procedures. This condition will be met, in particular in the case of supply and service provision contracts;

- *Compliance with legal obligations:* when processing is necessary to comply with a legal obligation. This includes, for example, the communication of data to public bodies pursuant to a legal obligation; including public bodies (national and EU), tax, police, or judicial bodies;
- *Legitimate interest*: when processing is necessary for the pursuit of legitimate interests of AIM Cancer Center or third parties, without harming the rights and freedoms of its customers and/or users.

3.2 Purposes for which AIM Cancer Center processes personal data

Personal data collected by AIM Cancer Center is only processed for specific, explicit, and legitimate purposes. Whenever personal data is collected, it is used exclusively for the purposes expressly identified at the time of collection.

The main purposes that justify the collection and processing of personal data by AIM Cancer Center are:

- Drafting, negotiating and executing contracts with clients, employees, service providers, suppliers, users and others;
- Management of events promoted by AIM Cancer Center;
- Dissemination of newsletters;
- Physical Security of Facilities and People;
- Necessary to institute or maintain legal proceedings or to defend legal action;
- Necessary to prevent fraud or other illegal activities, such as intentional attacks on AIM Cancer Center's information technology systems.

3.3 Collection methods

AIM Cancer Center only collects personal data that is adequate, relevant and limited to what is necessary for the purposes for which it is processed.

Data collection must be done in writing, on paper (namely through forms and contracts validated for this purpose), or digitally via email, message, WhatsApp form via link and AIM Cancer Center social networks and in accordance with the procedures attached to this policy.

As a general rule, AIM Cancer Center collects personal data directly from each data subject.

3.4 Types of data subjects

In order to carry out AIM Cancer Center's duties, data from the following types of individuals may be collected and processed:

- Customers and their employees;
- Users;
- Service providers and their employees;
- Candidates and interns;
- Participants in events promoted by AIM Cancer Center;
- Visitors to the AIM Cancer Center facilities.

3.5 Categories of personal data processed by AIM Cancer Center

To carry out the different purposes described in 3.2, AIM Cancer Center collects the following types of personal data:

- identification data (such as name, place of birth, citizen card or date of birth);
- physical characteristics data (such as height, weight, age or gender);
- behavioral data (such as eating or exercise habits);
- medical and health data (such as pathologies, treatments or test results);
- personal situation data (such as household composition or their ages);
- contact details (such as mobile phone, address or email);
- qualification and professional status data (such as education level and CV);
- banking, financial and transaction data (such as IBAN or tax identification number);
- location data (such as IP address);
- images collected through video surveillance systems, without prejudice to current legislation.

4. Data subject rights

4.1. **Information Duties**

By legal requirement, data subjects must be provided with a set of information regarding how data is processed by AIM Cancer Center.

Such information must be provided at the time of data collection (where possible) or, if the personal data has been obtained from another source, within a reasonable timeframe, in a clear and accessible manner, in accordance with the principle of transparency.

In view of the type of treatments operated by AIM Cancer Center, the following information must be provided to the holders:

a) The identity and contact details of the person responsible for treatment (AIM Cancer Center);
b) The contact details of the data protection officer;
c) The purpose(s) of the processing for which the personal data are intended;
d) The legal basis for processing;
e) The legitimate interests of the controller or a third party (where applicable);
f) The recipients or categories of recipients of the personal data to whom the data may be communicated;
g) Possible transfers to third countries (if applicable);
h) Period for which personal data will be retained or, if this is not possible, the criteria used to determine this period;
i) The existence and form of exercising the rights of access, rectification, deletion, opposition, limitation of processing and portability;
j) If the processing of data is based on consent, the existence of the right to withdraw consent at any time, without compromising the lawfulness of the processing carried out based on the consent previously given;
k) The right to lodge a complaint with a supervisory authority.

4.2. **Form of provision of information duties**

All information described in the previous section is contained in the AIM Cancer Center's publicly available privacy policy, published on its website. Therefore, reference to this privacy policy should be made in all texts where this information is required.

In the various collection media (forms, contracts, or other), the data subject must be informed of the AIM Cancer Center's privacy policy. This is the document par excellence to which all data subjects should be referred for information, clarification of questions, or even to exercise their rights.

All updates to the AIM Cancer Center privacy policy are available on its website.

4.3. **Exercise of Rights**

Under current legislation, there are a set of rights that the respective holders can, at any time, exercise with AIM Cancer Center.

- *Right of access:* right that allows you to obtain information regarding the processing of your data and its characteristics (namely the type of data, the purpose of the processing, to whom your data may be communicated, retention periods and lawfulness of the processing).
- *Right of rectification:* right that allows you to request the rectification of data, requiring that they be accurate, current and complete.
- *Right to erasure of data or "Right to be forgotten":* right to request the deletion of data, when the data subject considers that there are no valid grounds for retaining their data and provided that this deletion is legally permitted (for example, it does not arise from the execution of a contract or compliance with a legal or regulatory obligation);
- *Right to Limitation:* the right to suspend processing or limit processing to certain categories of data or purposes. When the data subject exercises this right to restriction, their personal data will not be deleted, but may only be processed again with the data subject's express consent, or for the purposes of defending rights in legal proceedings or for reasons of public interest;
- *Right to Portability:* the right through which the data subject may request that their data be sent in a commonly used digital format, allowing for its reuse. Alternatively, the data subject may request that their data be transmitted to another entity that becomes responsible for processing their data. This right may only be exercised when the condition for lawful processing is the data subject's consent or the performance of a contract, and is also limited to automated processing;
- *Right of Objection:* right that allows the data subject to object to certain purposes (for example, object to marketing purposes). This right cannot be exercised where there are legitimate interests that prevail over your interests (for example, where the processing is necessary for the performance of a contract);

- *Right to Withdraw Consent:* the right that allows the data subject to withdraw his/her consent, but which can only be exercised when his/her consent is the sole condition of legitimacy;
- *Right to complain to the National Supervisory Authority*(CNPD).

4.4. **How data subjects can exercise their rights**

ANNEX I describes the procedure to be used for the exercise of rights by personal data holders, as well as the flow associated with the execution of their requests (including legally imposed response deadlines).

5. Processing of personal data

5.1. **Guidelines**

Without prejudice to applicable law, the disclosure of Personal Data, including informal sharing with other workers or collaborators, is prohibited.

When access to certain information requires a specific access profile, it must be requested in accordance with current procedures.

Personal data must be regularly reviewed and updated. If it is no longer necessary, it must be deleted, unless other conditions prevent such deletion.

All existing recommendations/procedures must be followed when using information systems (with special attention to issues related to the processing of personal data).

All processes containing personal data must be documented and known to the DIRECTOR OF OPERATIONS.

The transfer of personal data to third countries (outside the European Union) requires compliance with a set of specific rules. Whenever these situations arise, it is recommended that an opinion be obtained from the DIRECTOR OF OPERATIONS.

Whenever there is a need to enter into contracts or other legal texts where personal data is processed, previously approved drafts/models must be used or requested, with the knowledge of the DIRECTOR OF OPERATIONS.

Any request for clarification or opinion on data protection must be forwarded to the DIRECTOR OF OPERATIONS.

5.2. **Support means**

a) *Paper:* Documents containing personal data must be stored in areas and compartments that prevent access by anyone not involved in their legitimate processing. Controls to be implemented:

i. Procedure for controlling and accessing folders/documents containing personal data, especially when it involves sensitive personal data, including rules on access, use and subsequent return/storage of folders/documents;

ii. Checking for errors in the previous procedure (for example, ensuring that documents (originals, copies or printouts) are not left in areas where unauthorized persons may have access to them). Procedure for rendering documents (originals, copies or printouts) unusable, using paper shredders.

b) *Digital:* Digital information must be protected from unauthorized access, accidental deletion, and malicious cyberattacks. Controls to implement:

i. Information protection using robust authentication methods and access profiles;

ii. Encryption of all portable or removable storage devices (computers, disks, etc.);

iii. Creation of routines for storing these devices in safe places (closed cabinets, use of padlocks, etc.);

iv. Create the obligation to store all information produced in central systems and avoid local storage whenever possible;

v. Apply the procedures of the information systems in force to transfers of personal data outside the AIM CANCER CENTER, ensuring, in particular, the encryption of data;

vi. Eliminate all information on equipment removed from the asset, specifically through scrapping, in accordance with information systems procedures.

5.3 Physical access

Access by external persons to AIM Cancer Center facilities must be protected and controlled, particularly in places where personal data is processed (including access to computer systems or physical documents).

5.4 Logical access to personal data

Information containing personal data must be protected with specific and validated access, both in terms of access credentials and existing profiles. The use of logging systems is important to verify their effectiveness. Personal data cannot be accessed—read, copied, modified, or removed—without valid and authorized access.

5.5 Collection forms

Whenever personal data is collected through a form, the procedure in ANNEX II must be followed.

5.6 Documentation and registration of compliance

In order to comply with the legal obligation to demonstrate at all times compliance with this policy and its various procedures, the responsible areas must follow the procedures specified in ANNEX III.

5.7 Guidelines for database compliance

All Databases containing personal data must comply with the measures set out in this data protection policy.

5.8 Use of information systems

For the correct use of information systems, the various existing recommendations and procedures must be followed. Encryption of personal data (associated with access control) is one of the measures that provides greater protection in this regard and should therefore be used whenever possible.

6. Internal flows of personal data

Internal data flows are understood as the transfer of personal data between areas of the AIM Cancer Center.

An area may need certain personal data to complete a process and, to do so, requests the same from the area responsible for that personal data.

The transmission of personal data between different areas of AIM Cancer Center must be regulated and documented. Whenever this occurs, the procedures for regulating internal flows of personal data set out in ANNEX IV must be followed.

7. Data retention

The processing of personal data must comply with the principle of limitation of processing, i.e., the data must be kept until the end of the purpose for which they were

collected; after this period and if there are no other reasons that justify their retention for longer periods, the procedures defined, e.g., deletion or anonymization, must be carried out.

The procedures and principles applicable to data conservation are set out in ANNEX V.

8. Subcontracting Entities and Third Parties

This section addresses how the processing of personal data must be framed within applicable legislation, in the relationships that AIM Cancer Center establishes with other entities.

This framework involves identifying the type of entity (Subcontractor or Third Party), the formalization of contracts or other legal agreements containing specific and validated clauses on the processing of personal data, as well as how the transmission of such data will take place (including the need to identify whether this transmission occurs to third countries, outside the European Union).

The procedures to be followed by the responsible areas, in their relationship with other entities within the scope of personal data protection, are set out in ANNEX VI.

9. AIM Cancer Center Collaborators

The processing of personal data of AIM Cancer Center employees and collaborators always complies with the legal and regulatory provisions applicable to the protection of personal data.

The procedures and principles applicable to the processing of personal data of AIM Cancer Center workers and collaborators are set out in Annex VII.

10. Data breach

A 'data breach' is considered to be a violation of personal data, caused by a security failure that results in the unauthorized disclosure of personal data or its destruction/alteration.

A data breach can potentially have a number of significant adverse effects on data subjects, which may result in material or non-material damage.
It is therefore essential to adopt not only preventive measures aimed at avoiding situations of "data breach" of personal data, but also corrective measures that ensure immediate correction and minimization of the effects of a "data breach".

The procedures and principles applicable to the prevention and occurrence of “data breaches” are set out in Annex VIII.

11. Data Protection Impact Assessments (DPIAs)

Whenever new situations arise that may pose significant risks to the rights and freedoms of individuals, a Data Protection Impact Assessment (DPIA) must be conducted. The purpose of a DPIA is to assess and identify the risks of a given operation to the protection of personal data, allowing, on the one hand, the anticipation of potential constraints and, on the other, the adoption of measures that minimize or eliminate the identified risks.

The procedures and principles applicable to carrying out AIPD are set out in Annex IX.

ANNEX I: Procedure for exercising the rights of holders

1. Purpose and scope:

Data subjects must be able to exercise their rights in accordance with relevant national and EU legislation. This procedure aims to regulate how the request is collected and processed through to its completion.

2. Who is it for:

a) To the holders of personal data;

b) To employees who receive requests from data subjects;

c) To the areas responsible for executing the aforementioned requests.

3. Shape:

All data subject requests must be submitted in writing through the formal channel provided for this purpose. That is, whenever a data subject wishes to exercise their rights, they should be advised and directed to the AIM Cancer Center website's privacy policy page. This page provides all the information on this topic that may be useful to the data subject, as well as access to the contact information for the DIRECTOR OF OPERATIONS, where the requester can submit their request.

4. Order execution:

The reception and management of requests from holders is centralized in the OPERATIONS DIRECTOR, which are then forwarded to the areas responsible for their execution.

The request must be processed in all repositories containing the data subject's personal data and within the established deadlines (see 5. below). Execution of the request may be legally limited in certain situations. If in doubt, seek assistance from the DIRECTOR OF OPERATIONS.

Once the request has been executed, the responsible area must inform the DIRECTOR OF OPERATIONS of all actions taken and provide any clarifications he deems necessary.

The completion of the request is made by the OPERATIONS DIRECTOR with subsequent notification to the data subject.

5. Legal deadlines:

Requests from data subjects must be executed within a maximum period of 30 days (counted from the date of entry into the AIM Cancer Center system, until the date of response to the subject).

After this period, AIM Cancer Center is in breach of a legal provision, therefore, in case of doubt or if for any reason it is not possible to respond to a request within the timeframes described, the DIRECTOR OF OPERATIONS of AIM Cancer Center should be contacted, informing him of the reason for the breach.

ANNEX II: Procedure for forms collecting personal data

1. Purpose and scope:

This procedure aims to regulate the collection of personal data, through electronic forms defined by AIM Cancer Center.

2. Who is it for:

a) The departments responsible for the forms—i.e., those who define their content and/or request their publication, whether online or otherwise—are responsible for ensuring the implementation of these recommendations. They should coordinate with the relevant departments or entities responsible for their technical implementation.

b) The competent areas or entities whose mission is the technical implementation of the forms.

3. Prerequisites:

Use of tools in AIM Cancer Center information services.

The use of external platforms requires prior analysis and written regulations (formal agreements / contracts / "data processing agreements") in order to certify their compliance with national and community laws on the protection of personal data.

4. Rules for creating forms that process personal data

Typically, a web page that supports a form includes an initial informative text describing the intended objective and the reasons for collecting the information. This text should include a specific paragraph explicitly describing the specific, legitimate purposes for which personal data is collected/processed.

The collection of personal data must follow the principle of minimization, i.e., only the data strictly necessary for the intended processing should be requested.

Example of a form presented in an abstract way:

<Informational Text>

<Form:

Field 1 [ ) *

Field 2 ( ]

Field 3 ( ) >

If this is a form that collects personal data, it is necessary to add the following mandatory field at the end regarding the consent request (GDPR):

> [ ] I authorize the processing of the personal data collected in this form for the purposes described above. I declare that I have read and understand the AIM Cancer Center privacy policy.

NOTES:

- There must be a hyperlink in the privacy policy phrase to the corresponding page on the AIM Cancer Center website;
- The [tick-boxes] for these specific GDPR questions cannot be pre-filled. The data subject must take positive, informed, and unequivocal action;
- The text of the GDPR fields reproduced here should only be changed when there is a positive opinion from the OPERATIONS DIRECTOR to that effect.

5. Optional consents:

The various optional consent requests that are intended must be individualized and allow the refusal of those that the data subject deems appropriate.

Example:

[ ] I agree to receive newsletters or other information related to the activities of AIM Cancer Center.

6. Data transfer to third countries (outside the European Union):

Whenever there is or is a possibility of personal data being transferred to third countries (outside the European Union), the following text (or similar, depending on consultation with the OPERATIONS DIRECTOR) must be included in the description of the purposes:

"Your personal data may be transmitted to all entities involved in the management of the aforementioned program, even if they are located in third countries. In the latter case, this transmission may entail risks to your rights due to the lack of guarantees in these countries in relation to community and national regulations regarding the protection of personal data."

7. Technical implementation of forms

a) *Double Opt-In*: The "Double Opt-In" concept should be implemented whenever the legal basis is the direct electronic obtaining of the data subject's express and informed consent. For example, in cases of periodic disclosure of information by email.

The "Double Opt-In" concept, broadly speaking, involves ensuring that the email address entered in the form by the data subject is revalidated, i.e., by sending an automatic email to the data subject's mailbox requesting a positive and unequivocal action, which allows us to ensure that the email initially entered in the form is valid and managed by that data subject.

b) *Test record*: All forms must be associated with a set of records that ensures AIM Cancer Center can prove the data subject's consent. These records must contain the following information:

- Description of the Purpose for the processing of personal data;
- All form fields; in the case of GDPR consent request fields, save the text associated with each tick box;
- Date and time of registration;
- When using the "Double Opt-in" concept, the computer system must record, preferably in a database, the various interactions with the data subject, as well as save a copy of the emails sent and a record of the data subject's acceptance/consent (as this final acceptance action by the data subject is generally done by clicking on a URL or a button, the system may produce an internal control email with the date and time of consent and be saved together with the emails sent);
- AIM Cancer Center area responsible for the form;
- End date of data retention (from which deletion will take place);
- Other data that serves as proof of consent.;
- All these pieces of evidence must be properly safeguarded and access controlled.

8. Documentation

Each processing of personal data must be documented at a minimum. See the specific procedure on this matter for more information in ANNEX III.

9. Data retention period

Personal data must be deleted after the stipulated period.

It is the responsibility of the area responsible for processing to ensure compliance with the conservation/elimination deadlines as established.

For more information on this matter, see ANNEX V.

ANNEX III: Procedure for documentation and registration of personal data processing

1. Purpose and scope:

This procedure aims to regulate the documentation and recording of evidence associated with each processing of personal data.

Entities are required to keep a record of all personal data processing under their responsibility, which includes the following information:

- Type of data processed;
- Purposes;
- Description of the categories of data subjects and recipients;
- Security measures;
- Retention period;
- Legal basis (consents, contracts, others).

2. Who is it for:

Areas responsible for processing personal data

3. Shape - Digital

Each department must request support from the department responsible for information technology to create a subfolder named after the department within the "GDPR" directory of the AIM Cancer Center network department ("File system"). The request must indicate which employees have access to the subfolder and be notified to the DIRECTOR OF OPERATIONS.

3.1 **Digital folder content**

Each area responsible for processing must follow an organization for the type of data processing.

It is important to document each treatment succinctly and objectively, as mentioned in point 1.

Examples of some content:

- Documentation of the various personal data processing processes existing in each area.

- Proof of consent, when this was not obtained by automatic means (previously validated by the DIRECTOR OF OPERATIONS).
- Subcontractor agreements.
- Procedures associated with the processing of personal data.

3.2 **Consent**

Whenever data processing takes place where the basis for lawfulness is consent, it is extremely important for AIM Cancer Center to have the elements that allow it to be proven.

If consent is recorded digitally, using computer applications already adapted to meet this requirement, the evidence is automatically saved in the AIM Cancer Center systems (if in doubt, clarify with the area responsible for information technology or the DIRECTOR OF OPERATIONS).

For all other situations, all elements constituting the evidence must be placed in the folder referred to in point 3 above, including consents obtained on paper, where available. The originals must be kept in a protected and secure location and a digital copy must be kept in the aforementioned folder.

3.3 **Subcontracting contracts**

Whenever there is a new contract with Subcontractor type entities (see ANNEX VI), these must be kept in a protected and secure location, and a digital copy must be kept in the aforementioned folder.

ANNEX IV - Procedure for Internal Flows of Personal Data

1. Purpose and scope:

This procedure aims to regulate the internal flow of personal data between the different areas of AIM Cancer Center, i.e., the transfer of personal data between areas.

Certain processes may require personal data for their completion (for example, contracting health insurance for AIM Cancer Center employees, where the area responsible for the hiring process requires the area responsible for human resources to provide certain personal data of AIM Cancer Center employees).

2. Who is it for:

All areas of the AIM Cancer Center that may require access to personal data held in repositories to which they do not have access.

3. Responsible area:

Each repository/database has at least one responsible area, which is responsible for determining the purposes and means of such processing.

4. Way to operationalize:

The department requiring access to personal data submits a request to the department responsible for the same. This request must contain the following mandatory information:

- Area identification;
- Identification of employees in this area who need access to the data;
- Type of repository/database you want to access;
- Type of personal data to which access is requested (example: name, address, NIF, date of birth, among others);
- Purpose of access (explain why access to such data is needed);
- Data retention period (explain the period of time during which the data will be processed, with the commitment that it will be destroyed after that period).

The area responsible for personal data precedes the analysis of the request and validates its meaning based on the following criteria:

- *Adequacy*: the suitability of the purpose for which the data is requested by the third area must be analyzed;

- *Need*: it must be analyzed whether, in view of the purpose that dictates such access, there is an effective need for total or partial access to the personal data requested.
- *Proportionality*: in addition to the need, the responsible area must also verify whether access to such data is proportional to any potential risks to the rights, freedoms and guarantees of the holders.

The response from the responsible area must contain:

- Granting or denying access;
- Basis for the decision;

In case of approval, the following must also be mentioned:

- Period of use of the data provided;
- Any limitations or restrictions.

In situations where there is approval, access to the requested data can be carried out using one of the following methods:

1) Assign application access to the employees indicated in the request, auditable and limited to the personal data strictly necessary and for the time necessary.

2) Sending a file with this informationtion to the area that requested this data, through a shared logical folder in the AIM Cancer Center information system, which should only be accessed by the employees referred to in the request by the third area.

3) Sending the file by email; in this situationtion it is essential that the file is encrypted, and the password must be communicated by another means, such as telephone.

Sending files containing unencrypted personal data via email should be avoided (in order to avoid possible data breaches).

It is recommended that the Departments Responsible for Personal Data use a Ticket System to support and document these requests. Otherwise, all request documentation must be kept in accordance with ANNEX III.

5. Situations in which the DIRECTOR OF OPERATIONS should be involved

Depending on the type of data, the purpose for which it needs to be accessed, or the period for which the third party intends to retain it, it may be necessary to request an opinion

from the DIRECTOR OF OPERATIONS. It is the responsibility of the responsible department to make this judgment and, in case of doubt, to request said opinion.

The DIRECTOR OF OPERATIONS should also be consulted in case of doubt regarding the mandatory documentation that must be kept for each order.

ANNEX V - Procedure regarding the Preservation of personal data

1. Objective and scope:

All documents containing personal data must comply with the principle of limitation of processing with regard to their retention period.

Data must be kept until the end of the purpose for which they were collected, until the end of the legally imposed deadlines for the retention of such data or until the end of legal proceedings that justify their retention.

Each department must identify the maximum retention periods for each personal data processing process and establish procedures to be followed when these periods are reached. If in doubt, consult AIM Cancer Center's legal department.

2. Who is it for?

All areas of the AIM Cancer Center.

3. Retention/Archiving Periods (recommendation)

The definition of retention periods is made in accordance with the law or through internal procedures.

The following points serve as guidance and as such should always be validated with the responsible entities (e.g. community programme management authorities, internal legal department, etc.):

- Financial/tax commercial documentation: It must be retained for 10 years after the end of the commercial relationship. In this regard, when processing personal data of company contacts that are not necessary for accounting records, there is no legitimate reason to retain them after the termination of the contract, and they must therefore be deleted after the end of the contractual relationship.
- Labor Documentation: In view of the expiration periods and the different existing legal regulations, the following retention periods must be met with regard to the documentation of AIM Cancer Center employees:
    - Biometric data: must be kept only for the period necessary to pursue the processing purposes for which they are intended (attendance control) and must be destroyed after the end of the employment relationship or if the employee is transferred to another workplace (article 18, paragraph 3 of the Labour Code);

- Contractual and social security documentation (e.g. employment contract, documents relating to the termination of employment contracts, holiday schedules, work schedules, individual employee records, records of disciplinary sanctions, professional training plan and evidence of professional training activities, annual consultation with employees on matters of safety, hygiene and health in the workplace, communications of admission and termination of employment contracts) must be kept for at least 5 years after the termination of the employment contract;
- Documentation required for tax purposes (e.g. receipts, withholding taxes, AT reports) must be observed for a period of 10 years after the termination of the employment contract;
- Documentation relating to occupational health and safety: AIM Cancer Center must keep records relating to the performance of activities inherent to occupational health and safety at the disposal of the competent supervisory bodies for a period of 5 years after the end of the employment relationship (e.g. results of occupational risk assessments, list of sick leave situations and number of days absent from work, to be sent by the personnel department and, in the case of occupational diseases, the list of reported diseases, list of measures, proposals or recommendations formulated by the occupational health and safety service).
- Recruitment processes (curriculum vitae, application assessments, interviews): 5 years after the end of the recruitment process;
- Remaining personal data of AIM Cancer Center employees, not included in the previous categories (such as data on family members, driving licenses or others): must be anonymized or deleted within a maximum period of 10 years after the end of the contractual relationship.

- Video surveillance: Images collected through a legally installed video surveillance system must be kept for a maximum period of 30 days, after which they will be destroyed and may only be used in accordance with criminal and procedural legislation.
- Data inherent to training actions, missions or catalogs: If there is no specific legislation that determines the retention periods for this type of data, and making a judgment of necessity/proportionality inherent to them, such personal data of guests and participants must be retained for the period necessary to fulfill the

purposes for which the data were requested (except if there is some other purpose that requires a longer retention period, namely documentation necessary for tax purposes);

- Data inherent to generic purposes of AIM Cancer Center (newsletters, website, company contact files): Data may be stored for as long as the purpose for which it was collected continues, on the assumption that the right to erasure or withdrawal of consent can always be guaranteed.

ANNEX VI - Procedure for Subcontracting Entities and Third Parties

1. Purpose and scope:

The entities that interact with AIM Cancer Center, as those responsible for processing personal data, can be of two types:

- Subcontractors: public or private entity that processes personal data on behalf of AIM Cancer Center (data controller) and for the purposes defined by the latter;
- Third: public or private entity that processes personal data to achieve purposes arising from the exercise of its own activity, with AIM Cancer Center not determining the method or purposes of that processing.

The key difference between these two types of entities lies in the fact that the subcontractor processes personal data on behalf of and on behalf of AIM Cancer Center and in accordance with the latter's instructions.

It is AIM Cancer Center's responsibility to only use subcontractors who provide sufficient guarantees of implementing appropriate technical and organizational measures so that the processing meets the data security, integrity and confidentiality requirements imposed by the General Data Protection Regulation (GDPR), and ensures the defense of the rights of the data subject.

This specificity requires that the relationship with subcontractors must be regulated by a written contract that sets out how data processing is carried out and what measures the subcontractor adopts to ensure the security and confidentiality of the data processed.

Processors may not engage another processor (sub-processor) without the controller having given specific or general prior written authorization to that effect. However, general authorization may be granted for the engagement of sub-processors, with the processor being required to inform AIM Cancer Center in writing of the identification of such sub-processors (thus giving it the opportunity to object to any such engagement).

With regard to third parties, although they may have access to AIM Cancer Center's personal data, they process such data to achieve purposes arising from the exercise of their own activity, with AIM Cancer Center not determining the method or purposes of such processing.

2. Identification of Related Entities by type

By reference to the distinction established in the previous point, below is a list (non-exhaustive) of the types of entities to whom AIM Cancer Center communicates personal data, and the respective purpose of the communication:

- Subcontracting entities:
  - External consultants (for auditing or consulting purposes;)
  - Occupational Medicine Company (to provide occupational medicine services);
  - Insurance Broker (for managing employees' personal accident insurance);
  - Travel Agenda (for managing and booking travel and accommodation);
  - Recruitment entities;
  - Lawyers (sponsorship of legal actions);
- Third parties:
  - Social Security (for registration at SS district centers);
  - Employment Guarantee Compensation Fund (for registration in the FGCT and FCT);
  - Workers' Committee (for the purposes of legal attributions);
  - Courts and Enforcement Agents (management of remuneration seizure notifications;)
  - Training entities (for the purposes of training and issuing training certificates);
  - Airlines and hotels (for direct purchase of airline tickets and accommodation);
  - PSP and/or GNR authorities (for the purposes of managing administrative offence proceedings);

If you have any questions about the type of an entity, please contact the DIRECTOR OF OPERATIONS at AIM Cancer Center.

3. Contracting

Contracts with entities that may, through any form or medium, access personal data - subcontractors or third parties - must use approved and defined templates for this purpose (see templates provided by the Legal department).

The minutes for subcontracting entities require greater detail and should include text covering the following items:

- object of processing (specification of services provided),
- nature and purpose of the processing (specification of purposes);
- categories of data subjects;
- type of personal data (identification data, contact details, financial situation, qualifications, among others);
- technical and organizational measures to be used by the subcontractor in the processing of data, in particular measures for controlling access, provision, transmission and deletion.

It will be the responsibility of each responsible area to ensure that appropriate minutes are used.

Whenever contracts are concluded with subcontractors, as defined above, these must be digitized in accordance with ANNEX III and the DIRECTOR OF OPERATIONS must be informed of them.

4. Transmission of personal data to Third Parties

4.1 Order

It is the responsibility of each responsible area to analyze any requests for information that involve the transmission of personal data held in AIM Cancer Center repositories/databases.

This analysis must follow the following points:

- After receiving the access request, the responsible area must analyze whether the following mandatory information has been provided:
  - Identification of the Third Party;
  - Type of personal data whose access is desired (description of the data category - e.g.: name, email, NIF, among others);
  - Purpose (justification) and basis for legitimacy of access: compliance with a legal obligation (the respective legal basis must be indicated); public interest; or legitimate interest of the Third Party;
  - If such mandatory information is not provided, the responsible area must request such information from the Third Party. If such information is not provided, access to the data must not be permitted;

- After sending the mandatory information described above, the responsible area must analyze the request, based on the following criteria:
- Lawfulness: the existence of one of the conditions of lawfulness for access/communication must be analyzed (i) compliance with a legal obligation (the respective legal basis must be indicated); (ii) public interest; (iii) legitimate interest of the third party;
- Necessity: it must be analyzed whether, in view of the purpose that dictates access, there is an effective need for access, in whole or in part, to the personal data requested.

- If the request is granted, the following message must be included with the transmission of the information: "The information now sent is for the purpose of <Specify Which>. To the extent that the information contains personal data, it must only be used for the aforementioned purpose and not for any other purpose (for your own benefit or that of a Third Party), and must be treated in accordance with national and Community legislation regulating the processing of personal data."
- The recording of all requests for access/information and respective responses must follow the guidelines in ANNEX III.

4.2 Outside the European Union

The communication of data to entities located in third countries (outside the European Union/EEA - European Economic Area) requires a more rigorous procedure, with AIM CANCER CENTER only being responsible for transferring data to third countries or international organizations that provide adequate guarantees under the terms of the GDPR.

It is the responsibility of each responsible area to analyze the existence of these situations (data transfer to third countries) and, in case of doubt, consult the DIRECTOR OF OPERATIONS of AIM Cancer Center.

As a general rule, data transfers to third countries should only be made if:

- There is an adequacy decision by the European Commission in relation to that country;
- There are binding rules applicable to companies within the same Group;

- There must be a contract between the entities with standard data protection clauses adopted/approved by the European Commission.

If it is not possible to meet one of the aforementioned conditions (as would be the case in most situations), data may only be transferred to other entities if:

- The data subject has given his or her express consent to such transfer, after having been informed of the possible risks of such transfers due to the lack of an adequacy decision and appropriate safeguards;
- The transfer is necessary for the performance of a contract between the data subject and AIM Cancer Center, under the terms of that contract;
- The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject under the terms of that contract;

4.3 Transmission method

The way in which personal data intended for other entities is communicated is particularly important since sending information/data through means that do not guarantee security, or sending information/data to the wrong recipients, may jeopardize the security and confidentiality of personal data and generate a personal data breach incident (see ANNEX VIII).

It is therefore up to each employee to take the utmost care when communicating personal data to external entities, always prioritizing the form of communication that guarantees the greatest possible data security.

In order to mitigate security risks when communicating data with other entities, the following recommendations should be followed:

- Whenever possible, transmission should be carried out through the Portals of other entities (such as the Tax Authority or Social Security Portal);
- If it is not possible to communicate data via Portals, files containing the data must be sent in encrypted form with a password, in accordance with the recommendations of the information systems area.

ANNEX VII - Processing of Personal Data of AIM Cancer Center Employees

1. Objective and scope

This annex is intended to inform you about how the personal data of AIM Cancer Center Employees is processed.

For the purposes of this document, the term "employees" refers to workers (regardless of the type of employment contract: fixed-term, secondment, secondment) and interns.

The entity responsible for processing your personal data is AIM Cancer Center and as such, will always follow the legal and regulatory provisions applicable to the area of personal data protection.

2. Fundamentals inherent to data processing by AIM Cancer Center

AIM Cancer Center will process employees' personal data to the extent necessary for the execution of the respective contract and to comply with the legal obligations incumbent upon it with regard to that contract (such as communicating your data to tax authorities or entities providing occupational health and safety services), as well as based on AIM Cancer Center's legitimate interests in managing its contractual relationship (for example, to monitor attendance and safety).

3. Purposes for which the AIM Cancer Center processes personal data

Personal data collected by AIM Cancer Center is only processed for specific, explicit and legitimate purposes, and is exclusively intended for the purposes identified at the time of collection.

AIM Cancer Center collects and uses the personal data in question mainly to manage the execution of your employment contract (including purposes such as career management, training management, management and contracting of insurance and other benefits, payroll processing, management of access to AIM Cancer Center facilities and equipment, organization of business trips, compliance with obligations related to health and safety at work).

AIM Cancer Center may also process the personal data in question to comply with legal obligations (for example, communications with tax and social security authorities) and court orders, as well as to exercise or defend AIM Cancer Center's legitimate rights in court or within the scope of supporting projects that include the recruitment of staff.

4. Collection methods

AIM Cancer Center only collects data that is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

Data collection can be done orally or in writing (namely through the curriculum vitae, the employee's individual file, identification documents and the employment contract).

As a general rule, AIM Cancer Center collects personal data directly from each employee, and personal data may also be collected from third parties, in particular from medical fitness sheets issued by entities providing occupational health and safety services, in accordance with the law.

5. Categories of personal data processed by AIM Cancer Center

To carry out the purposes described above, AIM Cancer Center processes the following types of personal data:

- Identification datation such as name, photograph, gender and date of birth;
- Identification documentstion, such as the citizen card, passport, details relating to requests for visits, driving license, NIF and NISS;
- Contact details, such as address, mobile phone, email and contact details of people to contact in case of emergency and/or next of kin;
- Inherent details the functions performed, such as your position, professional category, place or places where you perform your duties, hours, seniority, evaluations, disciplinary records, absences and holidays;
- Information regarding academic and professional qualifications;
- Financial data, with for example salary level, withholdings and bank details;
- Information relating to pensions and other benefits, such as information relating to contributions to the pension scheme, subsidies, insurance and equipment provided or financed by AIM Cancer Center;
- Information related to the use of systems, facilities and equipment provided by AIM Cancer Center, such as the ID of your computer and/or mobile or other devices, information about access to AIM Cancer Center facilities and CCTV footage;
- Health and safety information, such as records of workplace accidents, medical certificates and medical reports assessing fitness to perform duties.

6. With who does AIM Cancer Center share the personal data of employees

AIM CANCER CENTER only allows access to employees' personal data to those who need it to perform tasks and duties associated with contractual or legal obligations, as well as to third parties who have a legitimate purpose for accessing it.

Whenever access to personal data is permitted, appropriate measures are adopted to guarantee access only to the strictly necessary data, as well as the integrity and confidentiality of the data.

In terms of internal flow, in addition to the human resources area, responsible for managing AIM Cancer Center employee data, the personal data in question is only shared with other areas of AIM Cancer Center to the extent necessary (for example, for payroll processing purposes, to manage business trips or travel to fairs or other events).

In terms of data flow with external entities, certain personal data is made available to suppliers/subcontractors who provide services to AIM Cancer Center, based on necessity and in compliance with applicable legislation. For example, personal data is shared with third parties or subcontractors for the purposes of managing employee travel, arranging insurance contracts, archiving solutions (physical and digital), and occupational health and safety services.

Personal data may also be disclosed to third parties based on other legitimate reasons, such as, for example:

- To comply with the obligation legal obligations, including when necessary to comply with a legal regulation or court order (e.g. transmission of data to tax and social security authorities, as well as to courts and enforcement agents or the AIM Cancer Center Workers' Committee).
- When it is necessary for the purposes of the legitimate interests of AIM Cancer Center or third parties (including, in particular, public and ministerial bodies).
- When the transmission arising from the obligations inherent in the performance of duties under the employment contract.

For additional information about these third parties or subcontractors, please contact the department responsible for providing the data or, in case of doubt, the human resources department.

7. Shelf Life Data Collection

AIM Cancer Center will retain employees' personal data for up to one year after the end of the contractual relationship, except for data that, due to legal requirements, must be retained for longer periods.

AIM Cancer Center seeks to ensure that employees' personal data is maintained and, if necessary,

if so, securely deleted or destroyed, in accordance with existing policies, guidelines and rules on the retention of personal data.

8. Rights of personal data holders

Consult the Personal Data Protection Policy, Exercise of Rights.

ANNEX VIII – Procedure in case of Data Breach

1. Objective and scope

A "data breach" - for the purposes of applying the General Data Protection Regulation (GDPR) - is an intentional or accidental violation of personal data, which may lead to its destruction, loss, alteration, and unauthorized disclosure. It also covers situations where the confidentiality, integrity, and availability of such data are compromised.

The following examples constitute actual or potential situations of "data breaches":

- Unauthorized disclosure of data by hackers or due to protection/security failures;
- Transmission of a file containing various personal data of a group of AIM Cancer Center employees (for the purposes of this document, this includes workers and interns), in an unencrypted form, to an incorrect recipient;
- Theft or loss of equipment containing personal data repositories and not encrypted;
- Material that is considered obsolete/waste and that leaves AIM CANCER CENTER facilities, without any concern for making personal data contained in digital or paper media illegible, may lead to a "data breach" situation.

2. Who is it for?

All AIM Cancer Center employees.

3. Procedure to follow

<u>How should an employee proceed in the event of a "Data Breach" or suspected "Data Breach"?</u>

Whenever an employee becomes aware of or suspects an incident of this nature (see point 1), they must follow the following steps:

1. Always keep that possible, all supporting documentation or other evidence of the detected violation, as well as any exchange of communications on the subject (computer records, email exchanges, print screens, among others);

2. Report the incident to DIRECTOR OF OPERATIONS, within 24 hours, using the form at the end of this document. Please describe as fully as possible the breach detected and what personal data may be involved. Indicate whether any corrective measures have been taken and, if so, which ones;

3. Send the form and any information you deem relevant, to the DIRECTOR OF OPERATIONS at the email address dpo@aim.clinic, and establish a telephone contact after sending it in order to ensure the necessary speed, given that these situations imply the existence of very short legal deadlines.

4. The DIRECTOR OF OPERATIONS immediately analyzes the incident and ensures that the notification of the data breach constitutes or may constitute a personal data breach under the GDPR. If so, the DIRECTOR OF OPERATIONS takes the legally defined measures.

In the event that the incident constitutes a personal data breach:

1. On time within a maximum of 48 hours after detecting the data breach, the Administration or its legal representative determines that the areas of AIM Cancer Center involved, together with the DIRECTOR OF OPERATIONS, must identify the failures and risks in terms of the rights and freedoms of the data subjects.

2. THEAIM Cancer Center (Data Controller) must immediately implement measures to address existing flaws and minimize potential harm to the rights and freedoms of data subjects.

3. If it is concluded that the rape incident data breach affects the rights and freedoms of data subjects, the OPERATIONS DIRECTOR must, within a maximum period of 72 hours after the data breach incident, report the incident to the CNPD, using the online form available at www.cnpd.pt.

If the conclusion is that the data breach incident does not affect the rights and freedoms of data subjects, AIM Cancer Center is exempt from notifying the CNPD about such incident, and is only responsible for internally recording the incident (as well as the corrective measures adopted and consequent expected gains).

4. In the situation that the data breach incident poses a high risk to the rights and freedoms of individuals, AIM Cancer Center shall communicate the incident to the affected data subjects without undue delay and shall provide them with at least the following information:

- The name and contact details of the data protection officer and/or other contact point where further information can be obtained;
- To the likely consequences of the personal data breach;
- The measures adopted or proposed by AIM Cancer Center to repair the personal data breach, including, if applicable, measures to mitigate its possible negative effects.

Data Breach Reporting Form

1. Employee Identification

Name	
Area	
Contact	
Function	

2. Incident Information:

Time/Date of violation onset	
Time/Date of violation end	
Time/Date of knowledge of the breach	
How you became aware of the violation	

Type of violation:		Integrity (improper alteration)
		Confidentiality (improper access or disclosure)
		Availability (improper deletion)
Nature of violation:		Lost or stolen equipment
		Lost or stolen documents
		Lost or improperly accessed mail
		Hacking
		Malware
		Phishing
		Other
Cause of violation:		Non-malicious internal act
		Malicious internal act
		Non-malicious external act
		Malicious external act
		Other

Incident Description:

_____

_____

_____

_____

3. Consequences of violation:

Integrity

Can data alteration/corruption have consequences for data subjects? ☐ Yes ☐ No

Indicate which ones:	

Can data alteration/corruption be reverted to its original state? ☐ Yes ☐ No

Was the data encrypted? ☐ Yes ☐ No

Confidentiality

Can data alteration/corruption have consequences for data subjects? ☐ Yes ☐ No

Indicate which ones: ☐

Availability

Could the loss of data availability have resulted in consequences for the data subject (during the breach or in the future)? ☐ Yes ☐ No

Indicate which ones: ☐

Additional notes:

_____

_____

_____

_____

4. Personal Data:

Types of personal data:

☐ Identification data (Name, ID, NIF)
☐ Contact details (telephone, email, address)
☐ Financial data
☐ Sensitive data (e.g. health data)

Other data:

_____

Is it possible to determine the number of subjects involved? ☐ Yes ☐ No

Number of subjects involved: ☐

5. Data Subjects:

Holders of personal data

☐ Workers
☐ Clients
☐ Others

Additional notes:

_____

_____

_____

_____

6. Information for holders:

Were the holders informed of the breach? ☐ Yes ☐ No

Time/Date of violation report:	
Form of communication of violation:	
Number of holders contacted:	
Message sent to the holders:	

7. Preventive/Corrective Measures:

What measures were applied

ANNEX IX - Data Protection Impact Assessment Procedure (DPIA)

1. Objective and scope:

A Data Protection Impact Assessment (DPIA) is a process that aims to establish and demonstrate compliance with data protection principles. These assessments are an alternative to the prior authorizations issued by the CNPD, required by Law 67/98 of October 26 (LPDP) for certain types of personal data processing. They are provided for in Articles 35 et seq. of the GDPR.

Whenever a certain type of processing uses new technologies and, taking into account its nature, scope, context and purposes, is likely to entail a high risk to the rights and freedoms of individuals, AIM Cancer Center will first initiate a DPIA for the operations in question.

An AIDP must be carried out before starting the processing of personal data, and for this purpose it is essential to prepare a detailed description of the intended processing, so that it is possible to assess the necessity and proportionality of the processing in question.

When carrying out a data protection impact assessment, the controller requests the opinion of the data protection officer (DPO).

2. To whom it is intended

All areas of the AIM Cancer Center.

3. When should an AIPD be carried out?

There is only an obligation to carry out a DPIA when the processing is "likely to result in a high risk to the rights and freedoms of natural persons" (Article 35(1) of the GDPR).

The AIPD is mandatory, at least in the following cases:

- When carrying out a systematic and complete evaluation of personal data, based on automated processing, including profiling;
- When you treat each other, on a large scale, special categories of data (data relating to health, data revealing political opinions, religious or philosophical beliefs, or trade union membership, biometric data, etc.), or personal data relating to criminal convictions and offences;
- When a large-scale control is carried out system of public areas.

However, other operations may require a DPIA. It is therefore essential to identify and analyze the following situations in order to determine whether a given operation may pose a high risk to the rights and freedoms of individuals:

- Treatment of aspects related to professional performance, the situation economic situation, health, personal preferences or interests, reliability or behavior, location or movements of the data subject.
- Generation of automated decisions (i.e., without human intervention) that produce legal effects or significantly affect the data subject.
- Control systematic control of data, involving the observation, monitoring or control of data subjects, including data collected through networks, or a “systematic control of publicly accessible areas”.

• Processing of special data or data of a highly personal nature, such as data relating to racial origin or ethnicity, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health or data concerning sex life or sexual orientation, as well as personal data relating to criminal convictions and offences.
• Large-scale processing operations, considering the following factors as determinants of the existence of large-scale processing:
the. On number of data subjects involved, either as a specific number or as a percentage of the relevant population;
b. the volume of data and/or the diversity of different data to be processed;
w. the last action of the data processing activity or its relevance;
d. the geographical dimension of the processing activity.
• Data processing relating to vulnerable data subjects, considering as such those subjects who are not able to easily and freely consent or oppose the processing of their data or exercise their rights.
• Use of innovative solutions or application of new technological or organizational solutions that may involve new ways of collecting and using the personal data collected.
• Situations in which the processing itself prevents data subjects "from exercising a right or using a service or contract".
• Matches or combinations of data sets that exceed the reasonable expectations of the data subject.

Having analyzed all the aforementioned criteria, the greater the number of criteria met by the processing operation to be carried out, the greater the likelihood that it will pose a high risk to the rights and freedoms of data subjects and, therefore, require a DPIA, regardless of the security measures that the data controller adopts.

If you have any doubts in this regard, you should consult the DIRECTOR OF OPERATIONS at AIM Cancer Center.

Bridges to be detailed in an AIPD:
The AIPD should begin with a detailed analysis of the following items:
the) A systematic description of the operation and type of data processing, highlighting:
- The purpose of the processing;
- The grounds of legitimacy for such processing (e.g., the execution performance of a contract, compliance with a legal obligation or the legitimate interests of the controller);
- The duration of such operation;
- The media (physical or digital) on which the data may circulate;
- The area(s) responsible for the operation.

b) An assessment of the necessity and proportionality of processing operations in relation to the objectives (explanation of why data processing is necessary, making a judgment of necessity and proportionality);
w) An assessment of the risks to the rights and freedoms of data subjects - analysis of how the principles of confidentiality, integrity and availability of personal data to be processed are ensured and the risks that such principles may not be ensured; and
d) The measures envisaged to mitigate risks, including guarantees, security measures and procedures designed to ensure the protection of personal data and to demonstrate

compliance with the principles of confidentiality, integrity and availability of data, taking into account the rights and legitimate interests of data subjects and other data subjects.

ANNEX X - Personal Data Protection Procedure to be Adopted by Employees

1. Automatic passwords should be changed by the employee so that they are known only to him or her. They should be as complex as possible and changed frequently, even in systems that do not require this;

2. Passwords are personal and non-transferable, they should not be shared or written in places accessible to everyone;

3. The same passwords should not be used for the organization's systems and personal systems;

4. The worker must lock the computer whenever he leaves the room;

5. Applications and platforms containing personal data should not be left open on the screen if they are not being used;

6. Data storage devices (PEN, external hard drive) should not be left on the computer or in an accessible location if they are not in use;

7. Documents containing personal data should not be left near the printer and should not be torn up; these documents should be shredded using a paper shredder;

8. Employees should not leave documents containing personal data accessible on their desks. These should be stored in folders/files or in locked cabinets, preventing access by third parties.

9. If the employee loses his/her computer or work documents containing personal data, or suspects that a third party has accessed them, he/she must immediately notify the Data Protection Officer.

ANNEX XI - Personal Data Protection Procedure to be Adopted by the Human Resources Department

1. Access to each worker's individual file is only granted to the worker himself;

2. Workers' individual files are stored in locked cabinets, access to which is restricted;

3. Correspondence received by AIM Cancer Center is handled by a specific employee, and is subsequently distributed and/or archived on paper in a dedicated cabinet and on digital media in a restricted access folder;

4. THEAIM Cancer Center prefers to send correspondence containing personal data by registered mail with acknowledgment of receipt.