PRIVACY POLICY

1.- INTRODUCTION

1.1 – Objective

The objective of this policy is to define the commitment that **CATHMEDICAL CARDIOVASCULAR, SA** (hereinafter, **"CATHMEDICAL"**) with CIF **A81179772** and registered office at **C/Duero 37, local 15, CC El Bosque, 28670 Villaviciosa de Odón, Madrid** , must comply with in relation to the processing of personal data in the performance of its functions, and the framework in which said commitment is established.

1.2 – Scope of application

This policy applies to all professionals who are part of the CATHMEDICAL structure because they hold positions or are CATHMEDICAL staff with access to information for which CATHMEDICAL is responsible and may also be extended, in accordance with the data processing agreements that are signed, to any other company linked to CATHMEDICAL, whether a regular or occasional collaborator, whose actions may affect in some way the responsibility or reputation of CATHMEDICAL.

1.3 – Regulations

This document is based on compliance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation -GDPR) and current national legislation on the protection of personal data.

The regulatory framework applicable to the matter, which persons subject to this Policy must be aware of in addition to the aforementioned GDPR, is determined by:

- Organic Law 3/2018, of December 5, on the Protection of Personal Data and the guarantee of digital rights (LOPD and GDD).
- Law 34/2002, of July 11, on Information Society Services and Electronic Commerce (LSSI-CE)
- Royal Decree 311/2022, of May 3, which regulates the National Security Scheme in the field of Electronic Administration;

1.4 – Principles of data processing and information security .

CATHMEDICAL, its organizational structure and staff will process information and personal data under its responsibility in accordance with the following data protection and information security principles:

- Lawfulness, fairness and transparency: personal data will be processed lawfully, fairly and transparently in relation to the data subject.

- Legitimation in the processing of personal data: personal data will only be processed when such processing is covered by one of the grounds for legitimation established in articles 6 and 9 of the GDPR.
- Purpose limitation: personal data will be processed for the fulfillment of specific, explicit and legitimate purposes, and will not be further processed in a manner incompatible with those purposes.
- Data minimization: personal data will be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Limitation of the retention period: Personal personal data will be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data were processed.
- Integrity and confidentiality: Personal data will be processed in a manner that ensures its security, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, through the application of appropriate technical and organizational measures. Those involved in the processing of data will be bound by a duty of confidentiality even after the processing has concluded.
- Proactive responsibility: CATHMEDICAL and its structure will be responsible for compliance with the principles mentioned above and will adopt the technical and organizational measures that allow them to be in a position to demonstrate such compliance.
- Attention to the rights of the affected parties: measures will be adopted in the organization to guarantee the proper exercise by the affected parties, where appropriate, of the rights of access, rectification, erasure, opposition, limitation of processing and portability with respect to their personal data.
- Strategic scope: Data protection and information security must have the commitment and support of all organizational and management levels so that it can be coordinated and integrated with the rest of CATHMEDICAL's strategic initiatives to form a coherent and effective whole.
- Differentiated responsibility: In the information systems under the responsibility of CATHMEDICAL, the principle of differentiated responsibility will be observed in order to delimit the different responsibilities and roles.
- Comprehensive security: Security will aim to preserve the confidentiality, integrity, and availability of information, and may also encompass other properties such as authenticity, accountability, reliability, and non-repudiation. Security is understood as a comprehensive process comprised of all technical, human, material, and organizational elements related to the system, avoiding, except in cases of urgency or necessity, any ad hoc action or situational treatment.
- Risk Management: Risk management is the set of coordinated activities that CATHMEDICAL undertakes to direct and control risk. Risk is understood as the effect of uncertainty on achieving objectives, which, within the framework of the GDPR, is the protection of the rights and freedoms of the data subjects whose data is processed by CATHMEDICAL. Risk analysis and management are an essential part of CATHMEDICAL's data protection and information security process, enabling the maintenance of a controlled environment and minimizing risks to acceptable levels. These levels will be reduced through the deployment of security measures, which will strike a balance between the nature of the data and the processing activities, the impact and probability of the risks to which they are exposed, and the effectiveness and cost of the security measures. When assessing risk, CATHMEDICAL will consider the risks to the rights of individuals with regard to the processing of their personal data.
- Proportionality: CATHMEDICAL will establish protection, detection and recovery measures in a way that is proportionate to the potential risks and the criticality and value of the information, the processing of personal data and the services affected.

- Verification process: CATHMEDICAL will implement a process of regular verification, evaluation and assessment of the effectiveness of the technical and organizational measures to ensure the safety of treatments.

2.- OBLIGATION TO KNOW AND TO COMPLY

All CATHMEDICAL professionals must be aware of this Policy and act in accordance with the defined principles and behaviors, communicating to their direct supervisor or to the Compliance department within the General Secretariat Area any doubt regarding compliance or any indication of actions against it.

This Policy, as well as any subsequent procedures that may arise from it, will be permanently updated on the Intranet for later consultation when required.

All directors have the obligation to ensure compliance with the Policy in their areas, lead its implementation, resolve any doubts or concerns conveyed to them by professionals, and establish mechanisms to ensure compliance, relying on the advice of the Compliance department for all of this.

Questions about information security and data protection can be directed to the Information Security Officer, who, in turn, can forward them to the Data Protection Officer.

Failure to comply with the rules contained in this policy will be subject to CATHMEDICAL's disciplinary and sanctioning authority, in accordance with the principles and rules established by current legislation. Therefore, any significant concerns should be referred to the Information Security Officer, and any related non-compliance should be reported to CATHMEDICAL's Compliance Officer. The handling of concerns and non-compliance will be carried out in strict accordance with the principles of independence and confidentiality.

3. WRITTEN CONFIDENTIALITY AGREEMENT

Within the framework of the relationship that the company's employees will expressly commit to, in a document that they will sign, is to:

- Do not disclose to any person outside of CATHMEDICAL without their consent, the information to which they have had access in the performance of their duties, except in the case that it is necessary to give due compliance to the obligations of themselves or of the organization, imposed by the laws or regulations that are applicable, or is required to do so by mandate of the competent authority in accordance with the Law.
- Use the information referred to in the previous section only as required for the performance of your duties at CATHMEDICAL and do not use it in any other way or for any other purpose. Copying and sending any information obtained or generated as a result of your work for purposes other than work is prohibited.
- Do not use in any way any other information that you may have obtained by taking advantage of your status as an employee of the company CATHMEDICAL and that is not necessary for the performance of your duties at CATHMEDICAL.
- To comply in the performance of their duties at CATHMEDICAL with current national and community regulations relating to the protection of personal data and, in particular, REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April

2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and Organic Law 3/2018, of 5 December, on the Protection of Personal Data and Guarantee of Digital Rights (LOPDGDD),
provisions , applicable national regulations, or any other regulations that may replace them in the future.

- Comply with the Information Security Policies and its systems, as well as email and other communication systems, the procedures established and communicated to you by the Corporation's management.
- Do not make personal use of CATHMEDICAL's information systems and equipment in a way that interferes with the functions of other employees or the company within the CATHMEDICAL structure.
- On the internet, take appropriate precautions when downloading files, ensuring, before doing so, the trustworthiness or accreditation of the website from which it will be done.
- To fulfill the above commitments even after the relationship that binds you to CATHMEDICAL has been terminated, for any reason.

4.- USE OF CATHMEDICAL DIGITAL MEDIA BY EMPLOYEES

Employees must comply with the company's policies and instructions regarding acceptable use and security of information systems, email, and other communication systems, as established and communicated to them by management. They must not make personal use of CATHMEDICAL's information systems and equipment in a way that interferes with their own work, the work of other employees, or the company's operations. Employees will be informed that access to websites unrelated to work, such as chat rooms, non-professional social networks, games, gambling, travel, online shopping, stock trading, illegal or pornographic content, etc., is prohibited. The distribution and downloading of illegal or copyright-infringing material, as well as the illegal use, copying, or distribution of software or material protected by intellectual or industrial property laws, is also expressly prohibited.

On the internet, users should take appropriate precautions before downloading files, ensuring, before doing so, the trustworthiness or accreditation of the website from which the download will be made.

CATHMEDICAL may access the content derived from the use of digital media provided to the workers in order to monitor compliance with labor or statutory obligations and to guarantee the integrity of said devices.

Therefore, no CATHMEDICAL employee can expect their communications with CATHMEDICAL media or use of CATHMEDICAL computer systems to be confidential or private, as they are subject to the employer's control.

The employee will be informed that applications may be installed on company-owned computer equipment and systems that analyze internet traffic sent and received and allow or prohibit it based on a series of rules defined by the system administrators.

5.- EMPLOYEE MANUAL

The basic principles and obligations of employees will be set out in a document called the Employee Data Protection Manual, which will be distributed periodically to employees and updated.

6. INFORMATION SECURITY POLICY

Information security is governed by CATHMEDICAL's Information Security Policy in accordance with the security measures of the National Security Scheme, and a series of documents, procedures and development measures thereof (Security Regulations; Security Procedures; Authorization Processes; Security Measures of the Operational and Protection Framework), which the people responsible for its application must know.

The security of the systems will be attended to, reviewed and audited by qualified, dedicated and trained personnel in all phases of its life cycle: installation, maintenance, incident management and decommissioning.

CATHMEDICAL staff will receive the specific training necessary to ensure the security of information technologies applicable to CATHMEDICAL systems and services.

7.- DATA PROTECTION DOCUMENT SYSTEM

The CATHMEDICAL Data Protection Documentation System systematically compiles the documents generated by CATHMEDICAL, responsible for the processing of personal data and as the data processor, regarding the protection of personal data, in compliance with the General Data Protection Regulation (GDPR), national regulations and any subsequent legislation.

CATHMEDICAL, as the data controller responsible for processing personal data and in charge of other processing activities, is responsible for compliance with the principles of the GDPR and the LOPDGDD and the obligations incumbent upon it, and must be able to demonstrate this, in accordance with the principle of proactive responsibility.

The purpose of the Data Protection Documentation System is to demonstrate compliance with the GDPR and LOPDGDD.

The Data Protection Documentation System is under the custody of the Management Control Department and the Information Security Officer.

8.- PROCESSING OF PERSONAL DATA

8.1 – Content

“Personal data” means any information relating to an identified or identifiable natural person (“the data subject”). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number (e.g., national identity card number, social security number), location data (e.g., address), an online identifier (e.g., email accounts), or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person (e.g., biometric data). Hereinafter, “Personal Data”.

Examples of Personal Data would be the full name, ID or passport number, professional or personal address, nationality, profession, financial, health, genetic, biometric data, of an identified or identifiable natural person.

8.2 – Scope

It only applies to natural persons, since the aforementioned regulations would not be applicable to the data of legal persons.

8.3 – Data Format

For data to be considered personal, the format in which it is provided is irrelevant, whether it is electronic/digital format of any kind (Excel, Word, Access, PowerPoint, application, audio or video file, etc.), or physical format (paper document, photographs, etc.).

The security measures to be implemented will vary depending on the format in which the data is available.

8.4 – Record of Processing Activities – Use of data

CATHMEDICAL will keep the Record of Processing Activities updated with personal data for which it is responsible, which will include all the information referred to in Article 30 of the GDPR.

The purposes that enable the processing of personal data are those contained in each activity of the collection in the Record of Processing Activities.

The Record of Processing Activities will be kept continuously updated and can be consulted on the CATHMEDICAL website in accordance with the provisions of the LOPDGDD.

Any questions regarding the purposes of the processing should be directed to the Security Officer, or to the Data Protection Officer, if there is an obligation to appoint one.

Personal data must be adequate, relevant and not excessive in relation to the purpose for which they are collected.

No more data than necessary will be collected and personal data collected will not be used for purposes other than and/or incompatible with those for which they were collected.

8.5 – Authorization for data processing . Data collection . Obtaining consent

Processing is considered to be any operation or set of operations performed on personal data or sets of personal data, whether by automated means or not, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

It is understood that the processing of Personal Data exists from the moment such data is known or there is access to view it, even if it is a potential access (i.e., whether access is obtained or not, from the moment it can be accessed, the processing of Personal Data is taking place).

The authorization or legitimation for the processing of personal data will be based on one of the grounds for legitimation established in Articles 6 and 9 of the GDPR.

The specific authorizations for each of the treatment activities carried out by CATHMEDICAL are those included in the Register of Treatment Activities.

CATHMEDICAL will not collect personal data from users without their knowledge. The inclusion of data in forms will be voluntary and duly announced, with the relevant information clauses presented in two layers. The information layers and their levels of detail will have the content indicated in the Guide for Compliance with the Duty to Inform (2018) published by the Spanish Data Protection Agency.

Whenever data is collected, you will be informed in writing, or by recorded message if collected by telephone, with the first layer of basic information in table form, under the headings "Data Controller," "Purposes," "Legal Basis," "Transfers/Recipients," and "Rights." You will be informed that you can exercise your rights by emailing protecciondedatos@noxdata.es . The heading "Source" will be added, if applicable, only when the data does not come from the data subject themselves. The date of the clause version will also be indicated, and there will be an additional information link (+ info) to the Record of Processing Activities document.
Personal data that may be collected directly from the interested party in an informed manner will be incorporated into the corresponding processing activity owned by CATHMEDICAL.

When the legitimacy of the processing is based on consent and it is necessary to obtain it, the methods established in the Procedures for Obtaining and Storing Consent, which are part of the Documentary System for the Protection of Personal Data of CATHMEDICAL, may be used and the systems used in each case will be identified by processing activities, keeping the due record of the provision of consent, the data provided and the information clauses shown.

8.6 – Access method

For the purposes of processing Personal Data, the method of access (whether electronic/digital or physical) is irrelevant; therefore, the established procedure must be followed in all cases. Similarly, the processing of Personal Data occurs if access is gained by incorporating said data into CATHMEDICAL's computer systems or facilities .

8.7 – Security Level

CATHMEDICAL company employees must know and apply the security measures, in accordance with the National Security Scheme, which are included in the Register of Processing Activities and in the information security system.

To learn more about the levels of security regarding the protection of personal data, you should contact the Information Security Officer.

8.8 – Personal data processing and privacy policy for the website and internet

The Personal Data Processing and Privacy Policy for the website and internet, a document integrated into CATHMEDICAL's Personal Data Protection Documentation System, specifically outlines the

procedures governing CATHMEDICAL's processing of personal data through the website and internet, and the privacy of such data. This Policy also includes information on the use of cookies.
The Personal Data Processing and Privacy Policy for the website and internet must be known by the people of the CATHMEDICAL structure and will be published for general knowledge on the website.

8.9 – Data retention period Data blocking .

According to data protection regulations, personal data will be kept until it is no longer needed for the purpose of processing. The timeframes or criteria for each specific activity are recorded in the Record of Processing Activities.

They will subsequently be kept properly blocked. Blocking the data consists of identifying and reserving it, adopting technical and organizational measures to prevent its processing, including its viewing, except for making the data available to judges and courts, the Public Prosecutor's Office, or the competent Public Administrations, particularly data protection authorities, for the purpose of demanding accountability arising from the processing and only for the applicable statute of limitations. Once this period has expired, the data must be destroyed.

The blocked data may not be processed for any purpose other than the one indicated.

For the disposal of documents containing personal data, other than auxiliary copies, individuals within the CATHMEDICAL structure will consult with the Security Officer beforehand regarding the procedure to follow.

8.10 – Data Recipients

Data may be transferred or disclosed to other recipients as permitted by the GDPR. The specific transfers or disclosures are those recorded in the Record of Processing Activities for each activity, and all of them must be included in the information clauses and the consent form when consent is the legal basis for the processing.

8.11- Rights of interested parties

The rights recognized in Articles 15 to 22 of the GDPR may be exercised directly or through a legal or voluntary representative. Parents may exercise, on behalf of children under fourteen years of age, the rights of access, rectification, erasure, objection, or any other rights that may correspond to them under this Organic Law.

Anyone has the right to obtain confirmation as to whether or not CATHMEDICAL processes personal data concerning them.

Interested parties have the right to access their personal data and obtain a copy of the personal data being processed, to update it, as well as to request the rectification of inaccurate data or, where appropriate, to request its deletion when, among other reasons, the data is no longer necessary for the purposes for which it was collected.

In certain circumstances provided for in Article 18 GDPR, interested parties may request the limitation of the processing of their data, in which case only CATHMEDICAL will retain them for the exercise or defense of claims.

As a consequence of the application of the right to erasure or objection to the processing of personal data in the online environment, interested parties have the right to be forgotten according to the jurisprudence of the Court of Justice of the EU.

Data subjects may object to the processing of their data for marketing purposes, including profiling. In particular, data subjects have the right to request that CATHMEDICAL inform them, free of charge, that their personal data cannot be used for advertising or marketing purposes.

Under the right to data portability, data subjects have the right to obtain the personal data concerning them in a structured, commonly used and machine-readable format and transmit it to another controller.

Everyone has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them, except for the exceptions provided for in Article 22.1 GDPR. CATHMEDICAL does not process data by making automated decisions without human intervention.

The data subject has the right to erasure of their data, due to the disappearance of the purpose for which it was collected or processed, the withdrawal of consent when such consent is the basis for processing, or for any of the other reasons set out in Article 17 of the GDPR. In any case, definitive erasure will be carried out after the data has been blocked.

8.12 – Attention to the rights of interested parties

CATHMEDICAL has established a simple procedure for exercising personalized personal data protection rights, providing an email address for exercising these rights: protecciondedatos@noxdata.es , defined in the document "Procedure for handling the exercise of rights" which all CATHMEDICAL employees must know and apply.
Any request to exercise data protection rights received by CATHMEDICAL through any means or channel will be forwarded by CATHMEDICAL employees to protecciondedatos@noxdata.es . This policy will be included in the Data Protection Manual for employees.
Requests from interested parties will be answered by email with read receipt if the request has been received by that means, or by certified mail with acknowledgment of receipt if the request has been received by means other than email, without undue delay and no later than one month.

The burden of proof regarding compliance with the duty to respond to the request for the exercise of rights made by the affected party falls on CATHMEDICAL, therefore a copy of all responses and the justification of sending and receiving will be kept.

8.13 – Security breach management

The Procedure for managing security breaches, which is integrated into the Data Protection Documentation System, is established for the purpose of the correct identification, registration and resolution, with minimization of damage, of security breaches that affect personal data.

The breach management will be carried out according to CATHMEDICAL's Information Security Policy, which is governed by the documents that develop it and which cover aspects of prevention, detection and correction, to ensure that threats to information do not materialize and, if they do, do not seriously affect the information handled or the services provided by the company.

The existence of this Security Breach Management Procedure will be stated in the Data Protection Policy addressed to employees and any member of the company, who will be instructed on how to act in the event of security breaches and the responsibilities that correspond to them.

9. APPROVAL OF THE MODEL

9.1 – Ownership

Approval of this document is the responsibility of the company's management. The development and maintenance of this document is the responsibility of the Compliance department.

9.2 – Interpretation

The interpretation of this document is the responsibility of the Data Protection Officer in the company.

9.3 – Validity and review

This model will come into effect from the date of its approval and publication. Its content will be subject to periodic review, and any changes or modifications deemed necessary will be made.

10. DOCUMENT VERSION CONTROL

Version	File Name	Date
1.0	Privacy Policy	20/03/2026
1.1	Web Report	20/03/2026