GRANSOLAR GROUP

DATA PROTECTION POLICY

DOC N. º: GGR-CO-POL-0007
REVISION: A2
DATE: 17/12/2024

PUBLIC

Title	Data Protection Policy
Scope of Application	All Gransolar Group companies and subsidiaries over which the Group has effective control
Category	Policy
Elaborated by	Corporate Affairs Legal Department
Date of Approval	17/12/2024
Approved by	Board of Directors of Gransolar Group, S.L.
Version substituted	A1
New version	A2
Use	PUBLIC

Revision history

Revision	Date (dd-mm-aa)	Elaborated by	Changes made	Reviewed by
A1	27/01/2021	Corporate Affairs Legal Department	Implementation	Corporate Affairs Legal Department
A2	17/12/2024	Corporate Affairs Legal Department	Policy unification	Governance Dpt

Approvals

This document has been approved by

Name	Version
BoD 27/01/2021	A1
BoD 17/12/2024	A2

Index

*The Board of Directors of **Gransolar Group,** S.L. (hereinafter, **'Gransolar'**), as part of its general and non-delegable power to develop and approve the general policies and strategies of the company, has approved this Policy (hereinafter, the **'Policy'**).*

1. Introduction

At Gransolar we see policies and procedures as fundamental within our organisation, as they ensure compliance with rules and regulations, provide clear guidance on how to carry out different tasks and simplify internal processes.

At Gransolar we base our management on excellence, responding to the needs of our stakeholders, contributing value to society, and seeking social, economic and environmental sustainability. As Participating Members of the United Nations Global Compact, we promote the Sustainable Development Goals, assuming our role as an agent of change in terms of sustainability. Furthermore, Gransolar defends the recognition of Human Rights, adopting a defensive position in the face of possible violations in the territories where we operate, extending our Whistleblowing Channel to all our Stakeholders, updated in accordance with Directive EU 2019/1937 and Law 02/2023, in order to adopt standards of anonymity and confidentiality.

Furthermore, Gransolar is committed to the highest standards of transparency and accountability, following a zero-tolerance policy towards any conduct contrary to what is set out in our Corporate Policies and extending these commitments to all our stakeholders. This commitment, integrated in all its internal rules, is based on a corporate culture firmly rooted in the sustainability of the business model and extends to all the Group's operations and value chain.

Gransolar is convinced of its role as a leading agent of change. This is why we have adopted an 'early adopter' culture in relation to the new regulations recently approved by the EU, as well as the indications, guidelines, and recommendations of recognised international bodies.

2. Aim & Purpose

The present **Personal Data Protection Policy** (the "Policy") describes the rules and procedures that must be taken into account in the processing of personal data within the companies of the group headed by Gransolar Group, S.L. (the "Group"), with the aim of ensuring compliance with the applicable data protection regulations and being in a position to prove it.

In relation to the regulations applicable to this Policy, in addition to any other regulations that may be applicable in each case, the Group must comply with the following:

- Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016, on the protection of natural persons about the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (the "General Data Protection Regulation").
- Organic Law 3/2018, of December 5, on Personal Data Protection and Guarantee of Digital Rights (the "Organic Law on Data Protection").

This Policy is complemented by the Data Protection Procedure, which will establish the specific obligations and procedures to be followed within the Group, at all times, in this area.

3. Scope of application

This Policy applies to all employees and departments of the companies within the Group where control over operations is exercised by holding the majority of voting rights.

4. General Considerations in Data Protection

What are personal data? Personal data is any information about an identified or identifiable natural person, whose identity can be determined, directly or indirectly, in particular by means of an identifier (for example, an image) or by means of a set of information, which when collected can lead to the identification of a specific person (for example, the name of the company and the position of an employee). Data of legal entities (such as the tax identification number (N.I.F.), the corporate name, or registry data) and data of deceased persons are excluded.

Who is the data controller? The natural or legal person, public authority, service, or other body that, alone or jointly with others, determines the purposes and means of processing personal data. For example, when any of the entities that make up the Group acts as an employer, that entity will act as the data controller with respect to the personal data of its employees.

Who is the data processor? The natural or legal person, public authority, or body that processes personal data on behalf of the data controller. This is the case of companies, such as management firms or IT maintenance companies, that provide a service to the Group, for which it is necessary for this third party to access and process personal data for which the Group is responsible. The data processor only accesses and uses the personal data to provide a service to the data controller and does not use them for its own purposes.

Who is the data subject? This is the natural person identified by the personal data being processed.

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

What is a supervisory authority? An authority that is legally empowered to supervise compliance with data protection regulations and to correct any deviations that occur. In the case of Spain, the national supervisory authority is the Spanish Data Protection Agency ("AEPD").

What is the processing of personal data? Any operation or set of operations performed on personal data or sets of personal data, whether or not by automated means, 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. In short, any use or action on personal data will be considered the processing of personal data.

What is a file? Any structured set of personal data, accessible according to specific criteria, whether centralized or distributed functionally or geographically.

Who is the Data Protection Officer? The person or persons within the Group designated to coordinate, manage, and control, within the Group, the measures to ensure compliance with personal data protection regulations.

5. Scope of Application

5.1. Objective Scope of Application

This Policy applies to the collection and processing of personal data by the Group.

5.2. Subjective Scope of Application

This Policy is directed to and is mandatory for all persons who meet the following conditions:

i. Are linked to the Group by means of an employment or commercial contract, training agreement (internships, further studies, etc.) or, in general, any other type of analogous legal relationship, in which they perform functions as an employee or on behalf of the Group.
ii. In the performance of their duties and obligations, have authorized access to the Group's equipment, systems, internal and external communication networks, tools, applications or programs that are part of the Group's information systems, or to paper documentation containing personal data.

Hereinafter, the "Users". Users are required to comply with the procedures described in this document. Otherwise, the Group may hold the user legally or disciplinarily liable for non-compliance. For these purposes, Users are informed that this Policy and its subsequent updates or versions will be accessible at all times through the intranet or website.

5.3. Geographical Scope of Application

This Policy applies to all employees and departments of the Group's European companies.

6. General Rules for the Processing of Personal Data

6.1. Principles Relating to the Processing of Personal Data

Any processing of personal data carried out within the Group must comply with the following principles:

a) Lawfulness, fairness, and transparency: Personal data shall be processed lawfully, fairly, and transparently in relation to the data subject.

b) Purpose limitation: Personal data shall be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes, unless the data subject has given explicit consent for this additional purpose or there is another legal basis in accordance with applicable regulations.

c) Data minimization: Personal data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed, without collecting personal data that is not necessary. This means that personal data should only be processed when it is necessary for the intended purposes and, even then, only the data that is absolutely essential for that purpose should be processed.

d) Accuracy: Personal data shall be accurate and kept up to date and shall be erased or rectified without delay when the Group becomes aware that they do not meet this requirement.

e) Storage limitation: Personal data shall 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 are processed. When personal data are no longer necessary or relevant, they must be deleted. The head of each department must ensure that, within the specified time periods (see Data Protection Procedure), the data processed in that department is deleted, informing the department that manages the Group's databases. However, before the personal data is effectively deleted, the department that manages the Group's databases will first proceed to block it. Blocking involves identifying and reserving the personal data, adopting internal technical and organizational measures to prevent it from being viewed or processed, except for making it available to the competent authorities when necessary.

Once the statute of limitations for potential liabilities as dictated by the applicable regulations in each case (tax, accounting, labour, civil, etc.) has expired, the personal data must be deleted. To determine the applicable retention periods in each case, the Personal Data Retention Period, attached to the Group's Data Protection Procedure, must be consulted. Additionally, the relevant department head should be consulted, and in case of doubt, the Group's Legal Department should be consulted.

a) Integrity and Confidentiality: Personal data shall be processed in a manner that ensures its security, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organizational measures.

The Group is legally responsible for ensuring compliance with these Principles. All Users must observe them. To demonstrate compliance, proactive measures will be adopted as indicated below and as developed in the Group's Data Protection Procedure.

6.2. Lawfulness of Personal Data Processing

Personal data may only be processed within the Group if one of the following circumstances applies:

When the data subject has given their unequivocal (not tacit or presumed) consent to the processing of their personal data for one or more specific purposes. The Group must be able to demonstrate that it obtained the data subject's consent, so the physical support or corresponding digital evidence must be kept.

The data subject can withdraw their consent at any time, and the Group must provide a simple procedure for this purpose.

a) When the processing is necessary for the performance of a contract to which the data subject is a party or for the implementation of pre-contractual measures (for example, the Group's processing of its employees' data within the framework of the employment relationship).
b) When the processing is necessary for compliance with a legal obligation (for example, the communication of employee data to the Tax Agency or Social Security, by legal mandate).
c) When the processing is necessary for the purposes of the legitimate interests pursued by the Group or by a third party, provided that such interests are not overridden by the interests or fundamental rights and freedoms of the data subject which require the protection of personal data.

The Group must inform clearly and sufficiently about the legal basis for the processing of personal data, and also when it is going to transfer the data to third parties. In such cases, it must analyse the sufficiency of this basis before transferring the data and keep a written record of the elements that allow it to be accredited.

6.3. Processing of Special Categories of Personal Data

As a general rule, the processing by the Group of 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 aimed at uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation, is prohibited. Any new processing of special categories of personal data that is to be carried out within the Group, if applicable, must be previously consulted with the Data Protection Officer.

6.4. Principle of Proactive Responsibility

The Group is obliged to implement appropriate technical and organizational measures to ensure and demonstrate compliance with its data protection obligations. This is referred to as the "**Principle of Proactive Responsibility**." The measures outlined in this Policy allow for the fulfilment of the "**Principle of Proactive Responsibility**." Compliance with these measures must be reviewed at least once a year, making the necessary updates. The reviews and updates will be carried out by the **Data Protection Officer**.

7. Obligations of the Data Controller

7.1. Information to the Data Subject about the Collection of Their Personal Data

At the time of collecting personal data, the data subject must be informed about the conditions under which their data will be processed and the rights they have (principle of transparency). This information must be provided in writing, in a concise, transparent, intelligible, and easily accessible manner, using clear and simple language.

The obligation to inform data subjects about the circumstances related to the processing of their data lies with the Data Controller.

To comply with the duty to inform, the clauses or notices that facilitate the aforementioned content and have been prepared for this purpose will be used. Users must follow the steps below to verify that the legal clauses are being used correctly:

- In contractual relationships, use the personal data protection clause related to the right to information in the relevant contract, as established in the Group's Data Protection Procedure.
- Relationships between the Group and employees: See the relevant section of the Group's Data Protection Procedure referred to as "Processing of personal data of candidates and employees."
- On the Group's websites: See the section of the Group's Data Protection Procedure applicable to the processing of personal data on websites.
- In cases of video surveillance: See the Group's Data Protection Procedure in the section related to "Processing of personal data for surveillance purposes using cameras."
- In other cases: Consult with the Data Protection Officer to establish the appropriate clause or legal notice.

7.2. Conditions for carrying out the treatment

In the processing of personal data carried out by the Group's companies, a series of guidelines and conditions must be followed to ensure that this processing complies with the provisions of the current data protection regulations.

In this regard, we distinguish between different types of processing:

7.2.1 Processing of Personal Data of Candidates and Employees

In the collection and processing of personal data within the framework of selection processes and personnel management, a series of guidelines must be followed in accordance with current regulations. The description of these guidelines can be found in the relevant section of the Group's Data Protection Procedure. In cases where the Group's companies enter into agreements with universities for internships or contract with an external company for the provision of prevention services, they must first ensure that these agreements comply with the applicable regulations. Guidelines in this regard are provided in the Group's Data Protection Procedure.

7.2.2. Intercompany Agreements

In cases where there will be a reciprocal transfer and processing of personal data between companies within the Group, it will be necessary to regulate in writing the terms under which this access will occur, ensuring compliance with current data protection regulations. To this end, the contract for the reciprocal transfer and processing of personal data between entities provided in the Group's Data Protection Procedure must be followed.

7.2.3. of Data for Commercial Purposes

Whenever the Group wishes to use personal data for the sending of commercial communications, it must comply with the provisions set forth in the procedure called "Protocol for Sending Commercial Communications," as described in the Group's Data Protection Procedure.

7.2.4. Processing of Personal Data for Surveillance Purposes Using Cameras

The processing of personal data, especially images, as a result of the use of surveillance cameras is subject to certain specific rules. Group companies that carry out such processing must ensure that these processes comply with the provisions of the Group Gransolar Surveillance Policy, which is attached to the Group's Data Protection Procedure.

7.3. Data Processors

Sometimes, the Group hires other companies to provide services that involve the processing of personal data on behalf of the Group. These other companies are called data processors.

In such cases, guarantees must be required from the data processor through the signing of the Data Processing Agreement, which is provided in the Group's Data Protection Procedure.

The departments responsible for contracting suppliers will be responsible for ensuring that these Data Processing Agreements are signed in all cases where necessary. In case of doubt, the Data Protection Officer should be consulted.

Furthermore, the Group must only choose data processors that offer sufficient guarantees to implement appropriate technical and organizational measures, ensuring that the processing complies with legal requirements and guarantees the protection of the data subject's rights. Consequently, in cases where the data processor will carry out data processing that is quantitatively or qualitatively significant, their capacity must be evaluated by the departments responsible for the contracting. In cases where the supplier cannot demonstrate that they offer sufficient guarantees of compliance with the applicable regulations, they will not be engaged. In case of doubt, the Data Protection Officer should be consulted.

In cases where the supplier establishes data protection regulations in the draft contract they propose, such regulations must be verified by the Data Protection Officer.

7.4. Data Security

7.4.1. Implementation of Technical and Organizational Measures

The Group must implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk of the personal data processing it carries out. These **security measures** that the Group must adopt are described in the Group's Data Protection Procedure for consultation.

7.4.2. Notification of Personal Data Security Breaches

For the management, recording, and, if applicable, notification of security breaches, the Procedure for Responding to Personal Data Security Breaches will be applied, which is incorporated into the Group's Data Protection Procedure for consultation.

7.5. Duty of Confidentiality

The Group and all Users who access personal data must maintain confidentiality about them, even after the end of the relationship under which they became aware of the data, whether it is an employment relationship or any other type. To this end, Users must sign the User Confidentiality Agreement, attached as an annex to the Group's Data Protection Procedure. The People Department will be responsible for ensuring that this document is signed by Users, and it may be included as an additional item in employment contracts. In case of doubt, the People Department will consult with the Data Protection Officer.

7.6. Requests to Exercise Data Protection Rights

Data subjects whose data have been provided to the Group may exercise their rights of access, rectification, objection, erasure, portability, and restriction of processing at any time. The Group must facilitate the exercise of these rights by data subjects free of charge and respond to them in writing. If a request to exercise data protection rights is received from a data subject, it must be forwarded to the Data Protection Officer as soon as possible, indicating the date the request was received, so that the appropriate Group company can register and respond to the request in accordance with the GDPR. To this end, the Procedure for Responding to Requests to Exercise Data Protection Rights in accordance with the General Data Protection Regulation, which is attached as an annex to the Group's Data Protection Procedure, will be followed.

7.7. Privacy by Design and by Default

When the Group designs or initiates new activities or services that involve the processing of personal data, appropriate technical and organizational measures must be applied, both at the time of determining the means of processing and at the time of the actual processing, to ensure that only the necessary data is processed and only for the indispensable time. Furthermore, appropriate technical and organizational measures will be applied to ensure that, by default, only the personal data necessary for each specific purpose of the processing is processed. In order to comply with these principles, whenever new activities or services that involve the processing of personal data are designed or initiated, the responsible department head must be consulted beforehand. In case of doubt, they may consult the Data Protection Officer.

7.8. Cooperation and Management of Relations with the Supervisory Authority

The Group must cooperate with the Spanish supervisory authority (the Spanish Data Protection Agency or AEPD, in the case of Spain), whenever requested. When a request, requirement, or communication from a supervisory authority is received, it must be brought to the attention of the Data

Protection Officer in writing and immediately, so that a response can be provided or appropriate guidelines for the response can be given.

7.9. International Data Transfers

Whenever it is planned to carry out personal data processing that involves international transfers, this must be communicated in advance and in writing to the Legal Department, which will then inform the Data Protection Officer, who will provide the appropriate guidelines to ensure that the transfer complies with the applicable regulations. The international data transfer will not be carried out until it is confirmed that the conditions required by such regulations are met.

7.10. Data Protection Impact Assessment (DPIA)

When it is likely that a type of processing, particularly if it uses new technologies, due to its nature, scope, context, or purposes, entails a high risk to the rights and freedoms of individuals, a Data Protection Impact Assessment (DPIA) must be carried out beforehand. For this purpose, the Procedure for Conducting Data Protection Impact Assessments in accordance with the current Data Protection regulations, which is attached as an annex to the Group's Data Protection Procedure, must be followed. Whenever a new personal data processing activity is to be carried out or a substantial modification of an existing one is to be made, this must be communicated in advance and in writing to the hierarchical superior, so that they can inform the Data Protection Officer, who will advise on the necessity and conditions of conducting a DPIA.

8. Permitted Personal Data Processing Activities. Record of Activities

The Record of Processing Activities ("RPA") describes the personal data processing activities carried out within the Group. Users are not allowed to carry out personal data processing activities other than those indicated or outside the limits provided in the Record of Processing Activities, which is attached to the Group's Data Protection Procedure.

If a user deems it necessary to initiate a personal data processing activity different from those contemplated in the RPA or under different conditions than those provided, they must notify the responsible department head in advance via email and must not initiate the new processing activity until they receive confirmation that they can do so. The department head must consult this confirmation with the Data Protection Officer.

Whenever processing activities different from those included in the RPA are initiated, or existing ones are modified, the RPA must be updated. This update will be carried out by the Data Protection Officer based on the information received in accordance with the previous paragraph.

The Data Protection Officer will review the Group's Record of Processing Activities at least every 6 months.

9. Monitoring and Supervision Systems

The Legal department, and more specifically, the Data Protection Officer, will be responsible for coordinating and addressing data protection issues, in accordance with the guidelines and procedures included in the Data Protection Procedure.

The Data Protection Officer will be responsible for updating the Group's Record of Processing Activities at least every 6 months with the information provided by the different departments within the Group.

Additionally, the Legal department will periodically review and update the content of this Policy within a period not exceeding three years and will propose to the Board of Directors any modifications that contribute to its development and continuous improvement.

Avda. de la Transición Española 32

Parque Empresarial Omega, Edificio A

28108 Alcobendas (Madrid)

(+34) 917 364 248 **| group@gransolar.com**