



# **FI GROUP'S PERSONAL DATA POLICY FOR CLIENTS**



## Principal changes from the previous version

Versions	Date of creation or modification	Summary
V0	20/04/2020	Creation by the DPO TEAM
V1	19/10/2021	Modification considering the subcontracting ; non-substantial modifications and new branding

*"As FI Group is a worldwide company, it was given that appointing a Data protection for the whole group was a need. I have been then appointed in 2019 in order to ensure that all FI Group local entities are compliant with the personal data legislation and regulation. In order to achieve this goal, I am working in France with a dedicated team. Also, each country has its own « GDPR COMPLIANCE AMBASSADOR », who is the key contact and must adapt and implement my instructions. In 2020, my skills as a DPO have been AFNOR-certified (AFNOR has been certified by the French Data Protection Authority as per Article 42 of the GDPR). I truly believe that transparency is the key for a successful business relationship. Therefore, this policy shall help our future clients to understand what are the basics standards that I expect for each country. Do not hesitate to directly contact me if needed at : [dpo@fi-group.com](mailto:dpo@fi-group.com) and I will be very glad to give you the answers you need."*

Solenne DESPREZ BRAUN  
FI Group Data Protection Officer,  
AFNOR-Certified



**WHEREAS:**

- Since European Member States shall have the General Data Protection Regulation's (EU) 2016/679 (the 'GDPR') transposed into their National law, Portugal has implemented through the law named Law no 58/2019 on August 8, 2019, ensuring the execution of the GDPR in Portugal. These new provisions on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data imposes specific obligations on legal entities that processing Personal Data. FI Group has access to Personal Data as part of its business. FI Group shall act as a Data Processor and FI Group's clients shall act as a Data Controller.
- F-INICIATIVAS CONSULTADORIA E GESTAO LDA, with registered office in Rua da Alfandega, 108 1 esq 1100-016 LISBOA, registration number in the Vicenza Company Register and VAT number 508643759, represented by Mr. Frédéric Boute, as Chairman of the Board of Directors and legal representative is a company expert in engineering consulting and provides technical services to its clients as regards innovation financing through Research Tax Credits or public fund grants.

**NOW THEREFORE in consideration of the mutual covenants and agreements contained herein, the following terms must be understood as follows:**



# 1. INTERPRETATION AND PRELIMINARY

The headings of the provisions in this Policy are for convenience and reference only and shall not be used in the interpretation of nor modify nor amplify the terms of this Policy nor any clause thereof unless a contrary intention clearly appears.

- 1.1. **Data Controller** means the Client which processed Personal Data and which determines the purposes and means of the services provided by **FI Group**.
- 1.2. **Data Processor** means **FI Group** which processed Personal Data on behalf of the Data Controller.
- 1.3. **GDPR** means the General Data Protection Regulation (EU) 2016/679 of the EU Parliament and of the Council of 27 April 2016, on the protection of individuals through Personal Data protection which came into effect on May 25, 2018.
- 1.4. **Parties** meaning contracting parties which include the Data Controller and the Data Processor. No third party to the Service contract other than FI group and its client may invoke this Policy on Personal Data, which may only be invoked by the Parties.
- 1.5. **Personal Data breach** means a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data. It includes breaches that are the result of both accidental and deliberate causes.
- 1.6. **Personal Data Policy or "Policy"** means this Policy and how **FI Group** shall comply with the GDPR.
- 1.7. **Personal Data** means as per article 4 of the GDPR.
- 1.8. **Processing** means as per article 4 (2) of the GDPR. Refers to any operation or set of operations which are performed on 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.
- 1.9. **Sensitive Data** means as per article 9 of the GDPR. As a matter of principle, as defined by the GDPR, Sensitive Data do not have to be collected. In case of identification of Sensitive Data, the Personal Data provision within the Service contract shall be amended.
- 1.10. **Service contract** is the mission carried out by **FI Group** as part of the contractual commitment that requires Personal Data Processing.
- 1.11. **Subprocessor**: A third party appointed by the Data Processor to assist in the performance of the service and whose purpose is to generate Processing of the Data Controller's personal data, according to the Data Processor's instructions.

## 2. SCOPE OF THE PERSONAL DATA POLICY

Unless the Data Controller has given other written instructions, the Personal Data Policy shall apply for all Personal Data which are processed after the signing of the Service contract with **FI Group**. Through this Policy's Appendix, the Data Processor has listed all the essential information that the Data Controller shall know about the processing of Personal Data.

## 3. NATURE OF THE PROCESSING

- 3.1. The Data Processor hereby undertakes that the following principles are duly respected:
- Personal Data shall be processed only for a specific purpose and legitimate interest which is the execution of the Service contract.
  - Personal Data shall not be kept longer than needed.
  - Personal Data shall be kept in a safe and secure place.
  - Personal Data shall be provided only to the employees who truly need them in the course of their mission.
  - Personal Data shall not be sub-lease without the prior written consent of the Data Controller. If such authorization was granted, the processing shall comply with the Data Controller instructions.
- 3.2. Informing the data subject about the Processing is under the Data Controller's sole responsibility. The Data Processor shall be available to assist the Data Controller to elaborate an informative text.

## 4. AUTHORIZATIONS REQUIRED FOR SUBCONTRACTING

- 4.1. **FI Group** shall refrain from reproducing and/or transferring Personal Data outside the scope of its Services before the Data Controller has given prior written consent.
- 4.2. In the event that it is necessary to use subcontracting **FI Group** shall request written authorisation of the Data Controller. In the event of acceptance, **FI Group** undertakes to ensure that its processor complies with this Policy.
- 4.3. As an exception unless refused expressly by the Data Controller, it is however specified that **FI Group** may be required to use external solutions within the framework of the Service. External solution entailing the hosting of Personal Data with a service provider. As such, the solutions currently used by **FI Group** are the OFFICE 365 applications with OFFICE software (as

Outlook, PowerPoint, etc.) and online services (as One drive, Sharepoint, etc.) hosted by MICROSOFT company which is the Subprocessor for these applications. The Client may benefit from alternatives on simple request (data exchange platform hosted directly on the **FI Group** network, etc.). It shall be the responsibility of the Data Controller to give the necessary instructions and to warn its staff of the prohibitions relating to the use of certain tools, such as using and sending files through Teams. In addition, the conditions of compliance can be consulted here: <https://www.microsoft.com/fr-fr/trust-center/product-overview>.

- 4.4. The Data Controller undertakes to respond to **FI Group** within ten (10) working days of the above-mentioned requests for authorisation. **FI Group** shall consider that the Data Controller has accepted the request.

## 5. OBLIGATIONS OF THE DATA PROCESSOR

- 5.1. The Data Processor shall:

- Put in place appropriate security measures. The Data Processor shall make every effort to ensure that the security of the Personal Data complies with a level corresponding to the state-of-the-art in the field.
- Make its best efforts to report Personal Data breach to the Data Controller within 48 hours. Depending on Data Controller's instructions, it may inform data subjects under requested delays.
- Propose an adequate solution to fix the Personal Data breach as soon as it is discovered.

## 6. RETENTION AND DELETION

- 6.1. The Data Controller must communicate to the following address: [dpo-pt@fi-group.com](mailto:dpo-pt@fi-group.com), and / or FI Group's dedicated page on its website, which allows any data subjects to use their rights under chapter 3 (articles from 15 to 22) of the GDPR such as the right to access, rectification, erasure, data portability, etc.
- 6.2. The Data Processor must after verification of the data subject's identity, alert the Data Controller in a timely manner and waits for written instructions.
- 6.3. The Data Processor won't be able to delete any Personal Data if a statutory obligation requires to keep them on.

## **7. TERMINATION**

The Personal Data Policy shall apply as long as the Service contract applies. It may remain in force to the extent necessary, for provisions that shall survive including but not limited to storage limitation.

## **8. GOVERNING LAW AND JURISDICTION**

This Personal Data Policy is governed by and shall be construed in accordance with the law and jurisdiction as per the Service contract that has been signed by the Parties.





