FI GROUP POLICY FOR DATA PROCESSORS

Principales modifications par rapport à la version précédente			
Versions	Validation date	Editor	Modifications
V0	1st December 2020	DPO team	Creation
V1	1st October 2021	DPO team	New branding and adaptation

F-INICIATIVAS CONSULTADORIA E GESTAO LDA

Under number 508643759

Rua da Alfandega, 108 1 esq 1100-016 Lisboa

For any questions, do not hesitate to contact the referent to the personal data protection in Portugal : dpo-pt@fi-group.com or the DPO Group dpo@fi-group.com

1. INTRODUCTION

FI Group is a company specializing in the financing of innovation and committed to respect the obligations allowing the protection of personal rights.

Since the adoption of the General Data Protection Regulation (GDPR) n°2016/679 which entered into force on May 24, 2016, legal entities processing personal data must implement necessary means to be compliant with the GDPR entered into application on May 25, 2018 and its transposition into national law of each EU country.

Through the empowerment of persons who process Personal Data, the Regulation aims to strengthen the protection and rights of those affected by the processing of personal data.

Under this Regulation, FI GROUP that has access to personal data shall act as a Data Controller.
In its relations with service providers and/or suppliers whose missions require the communication of Personal Data they shall act as Data Processor.

In order to meet its own obligations, FI Group has the possibility to receive the assistance of its data processors, which must ensure the security of the personal data entrusted. As such, data processor can only process the data transmitted within the framework of the data controller's instructions without prejudice to specific provisions that could be signed besides.

The Data Controller's Policy purpose is to enable FI Group as data controller to communicate to its Data Processors the instructions to be followed for the use of the personal data entrusted.

2. GENERAL INFORMATION

ARTICLE 1 – DEFINITIONS

1. **Adequacy Agreement:** A status granted by the European Commission to countries outside the European Economic Area (EEA) who provide a level of Personal Data protection comparable to the level provided in European law. When a country has been awarded the status, Personal Data can pass freely between it and the EEA without further safeguards being required.
2. **Appendix to the Policy**: The Policy includes an appendix allowing the identification and description of the Personal Data entrusted as part of the Service provided for in the Contractual agreement. This Policy's Appendix is in principle incorporated into the contractual agreement and completed by the both data processor and FI Group.
3. **Contractual agreement**: A quote, a service contract or any writing in any form whatsoever describing the business relationship between the Data Processor and FI Group to which this Policy must be attached.
4. **Data controller or "FI Group":** In accordance with Article 4 of the GDPR a legal entity which determines the purposes and means of processing.
5. **Data Processing Register:** Inventory which lists all the Personal Data processed as well as all the useful information related to the data processing.
6. **Data processor**: Refers to the service provider which processes Personal Data on behalf of FI GROUP.
7. **Data Protection Law :** The national privacy or data security laws, including laws and regulations that apply to Personal data
8. **Detailed report:** On request of FI Group, report sent by the Data Processor to FI Group describing all the technical and organizational measures implemented by the Data Processor to ensure to Personal Data a level of security adapted.
9. **GDPR**: The General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 applicable since May 25, 2018.
10. **Personal data**: means as per article 4 of the GDPR
11. **Policy**: The data controller's Policy hereafter the "Policy".
12. **Processing** : Means as per article 4 (2) of the GDPR. Refers to any operation or set of operations which is 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.
13. **Security Breach Register**: Inventory which lists the description and the solution provided to a security breach.

14. **Security breach:** Weakness in the Personal Data protection security system allowing a person to undermine the integrity of this protection system, the confidentiality or the integrity of the protected data. A security breach does not automatically result in a Personal Data Breach.
15. **Service**: Tasks executed by the Data Processor at FI Group's request which require the processing of Personal Data.
16. **Simplified Report**: Means the summary drafted by the Data Processor in the event of a change in the method of securing Personal Data during the Assignment. The Data Processor describes the reasons and consequences of this change.
17. **Sub-processor**: A third-party used by a Data Processor to assist the Data Processor in its Personal Data processing under the instructions of the Data Controller.
18. **Supervisory authority**: The national data protection supervisory authority.
19. **Violation**: Unauthorized access to Personal Data or security risks which causes by accidental or unlawful manner whether the destruction, loss, alteration, unauthorized disclosure of transmitted Personal Data stored or processed in any way.
20. **Working day**: Day(s) from Monday to Friday inclusive, excluding statutory holidays.

ARTICLE 2 - PURPOSE OF THIS POLICY

The purpose of this Policy is to define the conditions under which the Data Processor undertakes to carry out on behalf of the Data Controller the Personal Data Processing operations entrusted as part of a Contractual agreement.

The data processor hereby certifies to respect current legislation and the instructions imposed by its Data Controller.

ARTICLE 3 - DURATION OF THE OBLIGATIONS

The Policy is intended to apply for the duration of the Contractual agreement.

At the end of the Contractual agreement, for any reason whatsoever the Data Processor shall undertake to:

- Archive only strictly necessary Personal data within the framework of the legal obligation. Once the legal deadline has expired the Personal Data must be destroyed, except for a return request which shall be made before the end of the statute of limitation, specifying the expected recording medium and format.

- Apply the above instructions to any sub-processors and to send archiving/destruction certificates for all Data Processor, also including its own certificates.

If no legal or regulatory obligation would require the Data Processor to keep the Personal Data by storage, the latter shall undertake to destroy them permanently at the end of all or part of the Contractual agreement or at the request of the Data Controller.
After the expiration of the Contractual agreement the obligations intended to continue shall remain in force.

Any change in the regulations in force relating to the processing of Personal Data, giving rise to a strengthening of the obligations of the Data Processor, shall be immediately implemented by the Data Processor who shall confirm these modification to the the Data Controller. It being understood that in the event of contradiction due to these evolutions, the Parties shall meet for the purpose of defining an amendment to the Policy.

3. INFORMATION AND INSTRUCTIONS ON THE PROCESSING OF PERSONAL DATA

ARTICLE 4 - PERSONAL DATA REFERRED BY THE POLICY

All the Personal Data communicated to the Data Processor under the Contractual agreement shall respect the Policy.

The Data Processor shall undertake to identify within a period of one (1) month after signing the Policy the type of Personal Data transmitted according to the template provided in Appendix 1.

Before any processing of Personal Data, the Data Processor shall verify that the Personal Data processed does not involve any risk for the freedoms and rights of individuals.
If the Data Processor, after having verified that the processing is not subject to a mandatory Privacy Impact Assessment (PIA) according to the list provided by the CNIL, considers that at least two criteria of the Protection Working Party (WP29) are met, FI Group must be informed of the reasonable doubt from the Data Processor. If FI Group considers that a PIA is necessary, the Data processor shall take necessary time to be part of it. Processing shall not start until the PIA is conclusive.

Likewise, if sensitive data within the meaning of article 9 or in connection with criminal convictions / infractions had to be identified the Data Processor undertakes to immediately notify FI Group before

starting the collection of Personal Data .
It shall also demonstrate that no other solution is possible and certify as quickly as possible notifying to FI Group in case of a Security Breach or Violation.

ARTICLE 5 - TRANSMISSION AND USE OF DATA

Under the Contractual agreement, the Data Controller shall communicate Personal Data of any kind and in any medium whatsoever to its Data Processor.

According to the principle of finality (purpose) only the data strictly necessary for the performance of the Service should be collected. As such, the Data Processor shall undertake according to the data minimization principle the collection of data to be requested from FI Group the minimum necessary information and using them only for the Service. Thus, the Data Processor shall not use the Personal Data for its own account, especially for the purposes of commercial, prospecting, marketing, statistics or other purposes.

The Data Processor guarantees that it acts only on "documented instructions" from the Data Controller and will immediately inform the latter if any of these instructions constitute a violation of a legal or regulatory obligation. An instruction from a Data Controller can be documented to the Data Processor by using any written form.

In the event that a Data Processor finds out that the Personal Data transmitted is not or no longer used shall undertakes after notifying the Data Controller to apply the same fate to that provided in Article 3 concerning the retention period of Personal Data at the end of the Contractual agreement.

ARTICLE 6 - INFORMATION AND CONTROL

Upon request from FI Group the Data Processor shall undertakes to provide within seven (7) Working days a Detailed report on the technical and organizational security measures implemented. In the event of a change in the security method the Data Processor shall undertakes to provide to FI Group a Simplified Report in the month following the modification.

In accordance with the GDPR, the Data Processor undertakes to keep a Data processing Register updated which must be made available to the CNIL. The Data Processor agrees to provide to FI Group its Data processing Register within seven (7) Working days following written request. This delay can be shortened in the request comes from a third party whose imposed delays are not compatible with the delay stipulated in the Policy.

In case of serious doubt about the veracity of these communicated elements FI GROUP reserves the right to ask its Data Processor for the communication of any document enabling ensuring the level of security in place.

In addition, in order to ensure that the technical and organizational measures put in place by the Data Processor are enough the Data Controller reserves the right to conduct audits within its office without ever exceeding one audit per calendar year.
The Data Controller shall inform the Data Processor Fifteen (15) days before the audit.
The Data Processor shall have the possibility to postpone the audit for fifteen (15) days if the date does not suit.
The Data Processor shall undertake to cooperate in such audits and more particularly to communicate all the information considered as reasonably necessary for the performance of this audit.
It is expressly specified that an audit report that does not reveal any irregularity is a determining condition for the continuation of the contractual commitment.
In the event of non-compliance noted in the audit report the Data Processor shall be able to present corrective actions within thirty (30) days from the submission of the audit report.
If these are sufficiently convincing for the Data Controller the Contractual agreement shall continue. If corrective actions are considered insufficient by the Data Controller the Contractual agreement shall be terminated by registered letter with acknowledgement of receipt without further formalism.

ARTICLE 7 - REQUIRED APPROVALS

1) REQUIREMENTS FOR SUB-PROCESSOR

In the exercise of its Service the Data Processor shall refrains using any other Sub Processors if at the time of the signature of the Contractual agreement was not working with any Sub Processors.

If it is necessary to have recourse to them the Data Processor shall provide the list of the concerned Data Processor(s) and request the written authorization from the Data Controller which reserves the right to accept or not. In the event of refusal by the Data Controller, the Data Processor may either (i) propose another Sub-Processor (ii) or propose once more the Sub-Processor who was initially refused by the Data Controller, by putting in before any corrective measures requested by the Data Controller. If neither of these possibilities is possible, the Data Processor will not have recourse to this Sub-Processor.

As an exception to the above conditions in the event that at the time of signing the Contractual agreement the Data Processor informed the Data Controller about using Sub Processors and provided the list of its Sub Processors concerned the access to the Data controller's Personal Data is authorized.

So, in the event of using Sub Processors under the aforementioned conditions the Data Processor shall undertakes to inform them about the Policy and shall undertakes to ensure that they must respect the Policy, being reminded that the Data Processor remains fully responsible to the Data Controller for the consequences of non-performance of the obligations incumbent on its Sub-Processors.

In the event of a modification of the list the Data Processor shall undertakes to notify of any change the Data Controller one (1) month in advance that may occur. Thus, FI Group may oppose the disclosure of its Personal Data to a new Data Processor. In case of deletion of a Data Processor from the list FI Group reserves the right to turn directly to the latter to give notice to respect the obligations linked to the end of the Service.

2) REQUIREMENTS CONCERNING THE PERSONAL DATA PROCESSING RELATED TO THE RIGHTS OF INDIVIDUALS

The Data Processor is prohibited from any reproduction and/or any transfer of Personal Data without the prior authorization of its Data Controller.

In this context, the Data Processor refrains from giving access, correcting, deleting or blocking Personal Data except with the express consent of the Data Controller.
In the event of a request from a natural person after having previously verified the identity of the concerned person the Data Processor shall undertake to transmit the request for access, correction or deletion to the Data Controller so that the latter can send the instructions needed to process this request within two (2) Working days.

ARTICLE 8 - EXCHANGE SECURITY

For all general questions relating to the processing of Personal Data, the Data Processor and FI Group may turn to the contacts identified in Appendix 1.

As part of the Service, the Data Processor and the Data Controller shall establish simultaneously with the signing of the Policy by the Data Processor a list of contact persons within their respective department to whom the Personal Data may transit.

In the event of a change of the list, the Data Processor and the Data Controller shall respectively inform each other in writing of this modification. The informed Party must acknowledge receipt of the information.

ARTICLE 9 - SECURITY MEASURES CHARGED TO THE DATA PROCESSOR

The Data Processor shall set up technical and organizational measures to ensure adequate security for Processing. It must at least provide:

Systematic locking of computer equipment holding Personal Data and left unattended.
The recurring change of passwords for all persons having access to Personal Data in the performance of the Service. This change must take place within a period in line with the criticality of the Personal Data.
A storage place with secure access as soon as Personal Data is communicated on a hardware support (paper, USB key, etc).

As an exception to the above, the Data Processor shall remain free to implement any security measures that these are at least equal to the measures referred to in this article.

The Data Processor shall undertake to respect and ensure the Personal Data confidentiality by its employees.

The Data Processor shall undertake to train its staff in securing Personal Data.

4. TRANSFER OF PERSONAL DATA OUTSIDE THE EU

ARTICLE 10 - THE PROHIBITION PRINCIPLE OF PERSONAL DATA TRANSFERS OUTSIDE THE EU

As a principle, the Personal Data transfer outside the EU is not allowed.

As an exception, countries benefiting from an Adequacy agreement according to the procedure referred to in Article 45 of the GDPR shall be considered as part of the EU and transfers shall take place without prior authorization. However, in case of changes leading to the abrogation of the Adequacy agreement, the Data Processor shall use the procedure referred to in Article 11 of the Policy.

ARTICLE 11 – EXCEPTIONS FOR TRANSFERRING PERSONAL DATA OUTSIDE THE EU

Transfer of Personal Data shall only be possible if cumulative conditions met:

- An interest within the execution of the Contractual agreement

- An express request - either through the Appendix when signing the Policy or through an update of the Appendix

- The transfer shall be protected by the appropriate measures referred to in Article 46 of the GDPR.

In the absence of appropriate measures as exhaustively set out by article 46 of the GDPR the Data Processor could demonstrate that the obligations of article 47 of the GDPR are fulfilled provided that the transfer is not repetitive and concerns a limited number of people.

5. INFORMATION AND INSTRUCTIONS IN CASE OF PERSONAL DATA SECURITY BREACH

ARTICLE 12 - PERSONAL DATA BREACH

In order to anticipate the implemented measures in case of Personal Data Breach, the Data Processor shall communicate to FI Group the method used if the risk is realized.

This method must be reported in the Detailed Report and if applicable the Simplified Report which shall automatically be returned in the event of a Violation. In support of this information, FI Group shall be able to assess the adaptability and effectiveness of the measures.

Within 24 hours following the Violation of a Personal Data the Data Processor shall undertakes to inform immediately the Data Controller of the implemented means through a Security breach register that kept up to date.

In the event of identification of a risk that could affect the security of Personal Data, the Data Processor shall undertake to notify FI Group within 72 hours. It being expressly specified that the Data Processor shall not free itself from any obligations to warn FI Group by taking advantage of a risk that has not occurred or of a "low" level of security breach.

As soon as the risk has been identified the Data Processor shall undertakes to implement immediately a corrective measure to achieve a more efficient level of protection than that initially planned in the event of a Personal Data Security breach.

6. SANCTIONS AND END OF THE SERVICE

ARTICLE 13 - SANCTIONS

In the event of default of one of its obligations under the Policy including but not limited to a subsequent Data Processor's default resulting in a financial penalty from the supervisory authority or any other legal entities empowered to sanction the Data Controller, the Data Processor shall undertake to reimburse to the Data Controller the sum that could not be attributed to the Data Processor's inconsistency.

In the event of an action, claim, demand or opposition from a third party linked to a default by the Data Processor to fully assume its responsibility and to reimburse the costs committed on proof to the Data Controller.

FI GROUP may demand the termination of the relationship with the Data Processor for any default of an essential and decisive obligation. Consequently, the immediate and automatic termination of the Contractual agreement.

ARTICLE 14 - END OF THE SERVICE

The Data Processor shall undertake to respect the obligations provided for in Article 3 and to issue an archiving/destruction certificate on first request within one (1) month following the end of the Service

The confidentiality obligation retains all its effects for an unlimited period following the end of the Service.

COMPANY:
Mr/Mrs:
Handwritten mention "good for agreement"
Date, stamp and signature