allfunds

GENERAL PRIVACY POLICY

- Version Control

Version	Date	Author	Changes
1.0	May 2018	Regulatory Compliance Unit	Initial Version
2.0	August 2019	Regulatory Compliance Unit	Version 1
3.0	Mayo 2022	Regulatory Compliance Unit Data Protection Office	Version 2

CONTENTS

1. REGULATORY FRAMEWORK

The General Data Protection Regulation[1] (hereinafter the 'Regulation' or 'GDPR"') tries to homogenise and harmonize the regulation on the protection of fundamental rights and freedoms of natural persons in respect of processing activities and to ensure the free flow of personal data between Member States. In this context, it introduced new legal provisions that address various aspects of data protection and privacy within a single framework for the European Economic Area.

Compliance with the Regulation requires to implement appropriated technical and organisational measures to ensure the security of personal data and recognise the protection of said data as a fundamental right.

2. GENERAL OVERVIEW

As stated in the GDPR[2] in Whereas (6), *'rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of the collection and sharing of personal data has increased significantly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Natural persons increasingly make personal information available publicly and globally. Technology has transformed both the economy and social life and should further facilitate the free flow of personal data within the Union and the transfer to third countries and international organisations, while ensuring a high level of the protection of personal data'*.

Therefore, it is required a strong and more coherent data protection framework backed by strong enforcement, given the importance of creating the trust in our stakeholders across the global market.

This Policy sets out the commitment of Allfunds Bank, S.A.U., including its subsidiaries, branches, and representative offices (hereinafter collectively 'Allfunds', or the 'Company'), with respect to privacy and protection of personal data, in accordance with the Regulation.

The purpose of this policy is to regulate the processing of personal data at Allfunds, regardless of the medium on which the data are processed, the rights of data subjects and the obligations of those who create or process the data. To this end, a single framework is established for defining privacy and the protection of personal data in which Allfunds undertakes to protect the personal data it processes always ensuring compliance with the different laws and regulations that apply on these matters.

[1] 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

[2] Terms used in this Policy correspond to the definitions set out in art. 4 of the GDPR.

3. SCOPE OF APPLICATION

This policy shall be supplemented and further developed by other corporate data protection procedures and shall apply throughout the Company, unless otherwise expressly provided by applicable local law.

Compliance with this policy is mandatory for the members of Allfunds management bodies and all employees, as well as for any person linked to Allfunds by a trainee or internship contract, or by a temporary contract through third parties (together hereinafter 'Relevant Persons') . Therefore, this policy and the rest of Allfunds ' rules and regulations on data protection matters will be available to them through the group intranet, and all Relevant Persons must know and comply with the same.

4. PERSONAL DATA

Personal data is considered to be any personal, numerical, alphabetical, graphic, photographic, acoustic or any other information concerning **identified or identifiable** individuals. In this context, an identifiable individual is any person whose identity can be determinated by means of an identifier (i.e. name, identification number or location data) or by using elements of the physical, physiological, genetic, psychological, economic, cultural or social identity of the natural person.

In accordance with GDPR, the processing of so-called special categories of personal data, which in addition to health data, include data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data, data concerning a natural person's sex life or sexual orientation and data relating to criminal and administrative convictions or offences, is only permitted under specific circumstances.

Before carrying out any activity involving the processing of personal data, Relevant Persons shall first contact the Allfunds' Data Protection Office, bearing in mind that the analysis is particularly important before carrying out any processing that impact in special categories of personal data.

5. PARTIES INVOLVED

The Company must ensure the security and integrity of all personal data which it processes directly as Data Controller, through the provision of services by third parties (third-party Data Processor) or as service provider to another enterprise (Allfunds as Data Processor). In all these cases, regardless of whether it acts as controller or processor, the personal data shall be controlled and their processing must comply with all required legal and contractual obligations and safeguards.

A. DATA CONTROLLER

Allfunds, as Controller, shall decide on the content, purpose and means of the personal data processing with respect to its counterparties, employees, and other data subjects. In carrying out these activities, the following instructions must be complied with:

- Ensure the data are appropriate and precise, legitimately obtained and processed in accordance with the purpose for which they were obtained.
- Ensure confidentiality in the processing of personal data.
- Inform the data subjects about the purpose of the processing activity in accordance with the applicable legislation, apart from to obtain their consent where applicable.
- Ensure that data subjects can exercise their rights and facilitate said exercise.
- Apply appropriate technical and organisational measures to ensure the protection of personal data and be able to demonstrate that the processing is in compliance with the Regulation. In addition, keep a record of the processing activities carried out under its responsibility and carry out privacy impact assessments where a particular processing operation is likely to result in a high risk to the rights and freedoms of natural persons.
- Notify any security breach regarding the protection of personal to the Supervisory Authority, if required under applicable law, as well as to data subjects where applicable.
- Ensure that personal data protection rules are respected in dealings with service providers or other third parties with access to personal data.

B. DATA PROCESSOR

Allfunds has service agreements with external providers who may have access to personal data. These providers shall process the data as Processors on behalf of Allfunds where the latter acts as Controller.

Similarly, Allfunds may act as Processor in the provision of services to another entity that acts as Controller.

In both cases the Processor shall ensure the Controller's fulfilment of its obligations, offering assurances that the processing will be carried out according to the applicable data protection legislation and to the relevant safeguards of the data subjects' rights. The adherence of the Processor to a code of conduct or a certification mechanism approved by a Certification Body or by the competent Supervisory Authority may be used as an element to demonstrate compliance with its obligations (as stipulated in articles 40 et seq. of the GDPR).

The processing of data by a Processor shall be governed by a contract between both parties (Controller and Processor) setting out the following:

- To process personal data only in accordance with the documented instructions of the Data Controller.

- Ensure confidentiality in the processing activities of personal data by the persons authorised to do so.

- Implement appropriate technical and organisational measures to ensure an appropriate level of security of the personal data, considering the nature of the processing.

- Require the prior authorisation from the Controller before engaging another processor as Subprocessor, unless otherwise provided by contract, and ensure that the conditions are fulfilled for the processing of personal data. In this case, the same data protection obligations shall be imposed on this Subprocessor as those stipulated in the contract between the Processor and the Controller.

- Permit and cooperate in all audits and inspections carried out by the Controller.

- Assist the Controller in responding to the exercise of the data subjects' rights and to ensure compliance with obligations related to security measures and privacy impact assessments.

- Delete or return personal data to the Controller at the end of the services, as agreed with the Controller, and delete existing copies.

C. SUPERVISORY AUTHORITY

Allfunds, as Data Controller, shall notify the competent Supervisory Authority of any data protection breach of which it becomes aware or consult with said authority before processing personal data whose privacy impact assessments result in a high risk to the rights and freedoms of data subjects.

With respect to the legal and contractual liability of both Controllers and the Processors, any breach may be subject to administrative fines or other sanctions, imposed by the Supervisory Authority.

D. DATA PROTECTION OFFICER (DPO)

The GDPR lays down the obligation to designate, in certain cases, a Data Protection Officer (hereinafter 'DPO') that is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

Allfunds has chosen to designate an internal Global DPO located in Spain within compliance department, who will be supported by the Data Protection Office, function undertaken by the Regulatory Compliance Unit, and by the local Compliance Officers in the different countries who report directly to the Global DPO in privacy matters. The GDPR Government Model procedure, published in the group intranet, establishes the government's requirements for privacy and protection of personal data and the role of the DPO within Allfunds.

6. FUNDAMENTAL PRINCIPLES

The applicable data protection regulations directly affect Allfunds 's operations, given that the Company processes personal data in its daily activity. The personal data will be processed according to certain principles and measures:

A. LAWFULNESS, PROPORTIONALITY AND TRANSPARENCY

Allfunds will process the data in accordance with the following:

- **Lawfulness**: the data must have been obtained lawfully according to the applicable legislation in each case.
- **Proportionality**: the data must only be processed for necessary, appropriate, and relevant purposes.
- **Transparency**: the information must be clear, exact, and unambiguous.

B. PURPOSES COMPATIBLE WITH THE INITIAL COLLECTION

Allfunds will ensure that personal data are processed only for the specific, explicit and legitimate purposes for which they were obtained and shall not be subsequently processed in a manner incompatible with those purposes, except with the data subject's due consent to carry on such processing.

C. MINIMISATION AND ACCURACY OF THE PERSONAL DATA

The personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. Furthermore, all reasonable measures shall be taken to ensure, if the data are inaccurate, that they be erased or rectified, considering the purposes for which they are processed.

D. STORAGE OF PERSONAL DATA

Allfunds will store personal data allowing the identification of the data subjects for a period no longer than necessary for the processing purposes in accordance with the applicable legislation and may keep them blocked for the time periods during which liability may arise for the Company.

E. INTEGRITY AND CONFIDENTIALITY OF PERSONAL DATA

Allfunds shall make sure that all data collected be processed so as to ensure their appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. For this purpose, there must be ensured a level of security appropriate to the risk, as well as the confidentiality, integrity, availability and flexibility of the systems and services.

In particular, the Company must ensure that its employees, third parties who provide services and the employees of such third parties who in the performance of their tasks have access to personal data for which Allfunds is Controller undertake to process the data in a confidential manner and refrain from sharing this data with third parties.

F. DATA PROTECTION BY DESIGN AND BY DEFAULT

Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing, as well as the risks posed by the processing to the rights and freedoms of natural persons, Allfunds shall implement, both at the time of determining the means of processing and at the time of the processing itself, appropriate technical and organisational measures in order to comply with the requirements of the Regulation and to protect the rights of data subjects.

Allfunds will apply measures to safeguard and demonstrate compliance with the legal requirements for data protection matters, by defining adequate procedures that are adapted to the specific circumstances of the Company Allfunds and that are properly designed and implemented, ensuring that they function properly in practice. A key factor in this regard is to implement data protection by design and by default:

- **Privacy by design:** When designing a product or service, the Company will consider from the outset issues regarding the protection of personal data, such as information requirements or obtaining appropriate consent for processing personal data of the data subjects and the technical and organisational measures necessary to protect such data taking into account the nature of the processing activity.

- **Privacy by default:** On a predetermined basis, only the personal data needed for achieving each of the specific purposes of the processing shall be processed, always ensuring the confidentiality of the personal data.

G. TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS

The GDPR defines an international transfer of data as any processing of data that involves transmission or access to the data outside the territory of the European Economic Area, whether as a communication of data or in the provision of a service.

Any transfer of personal data to a third country or to an international organisation shall take place only if an adequacy decision approved by the Commission exists or in case it is guaranteed and legitimated in all cases in accordance with the Regulation.

In this context, all Allfunds group entities have signed agreements aligned with the standard contractual clauses approved by the European Commission, thus ensuring an adequate level of protection in accordance with the Regulation for intra-group data transfers.

7. DUTY OF INFORMATION

Before collecting any personal data, the Controller shall inform data subjects about the different aspects related to the processing of their personal data in a in a concise, transparent, intelligible, and easily accessible form, using clear and plain language. The information shall be provided in writing or by other means, including, where appropriate, by electronic means, in accordance with the applicable legislation requirements.

Likewise, in accordance with the applicable legislation, Allfunds, as Data Controller, shall also inform data subjects when personal data have not been obtained directly from the data subject and are obtained through third parties.

8. LAWFULNESSOF PROCESSING

A processing activity shall only be lawful if;

- The data subject gave his or her consent to the processing of his or her personal data for one or more specific purposes.

  Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous will. In addition, Allfunds, as controller, shall be able to demonstrate that the data subject has consented to processing of his or her personal data. The data subject shall have the right to withdraw his or her consent at any time. Nevertheless, the withdrawal of consent shall not affect the lawfulness of processing based on consent prior to its withdrawal.

- Processing is necessary for the performance of a contract to which the data subject is part or for the implementation at his or her request of pre-contractual measures;

- Processing is necessary for compliance with a legal obligation applicable to the Controller;

- Processing is necessary for the protection of vital interests of the data subject or of another natural person;

- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller;

- Processing is necessary for the purposes of the legitimate interests pursued by the Controller 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, in particular where the data subject is a child.

9. RIGHTS OF DATA SUBJECTS

The Company shall inform all persons from whom it collects personal data of the risks, rules, safeguards and rights in relation to the processing of personal data and on how to exercise their rights. It shall also ensure that the data subjects can faithfully exercise their rights and receive responses in due time and form to their requests to exercise any of the rights of the data subject.

All interested parties in relation to whom Allfunds processes personal data may exercise the following rights by writing to this e-mail address: dpo@allfunds.com

- **Right of access**: Data subjects shall have the right to obtain from the Controller confirmation as to whether personal data concerning him or her are being processed or not, and if it is the case, to access to his/her personal data in order to establish and verify the lawfulness of the processing.

- **Right of rectification:** Data subjects shall have the right to obtain without undue delay from the Data Controller the rectification of any inaccurate or incomplete personal data concerning them, to ensure their accuracy and proper processing.

- **Right to restriction of processing:** Data subjects shall have the right to obtain from the Controller restriction of processing of their data, where any of the circumstances set out in the Regulation apply.

- **Right to erasure (right to be forgotten):** Data subjects have the right to obtain without undue delay from the Controller the erasure of personal data concerning them unless there is a legitimate ground for the Controller to retain the data.

- **Right to object:** Data subjects shall the right to object to the processing of their personal data at any time and without justifying this decision. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights, and freedoms of the data subject, or for the establishment, exercise or defence of legal claims.

- **Right to portability:** Data subjects shall have the right to receive the personal data concerning them and to request the transmission of their personal data to another controller, in a structured, commonly used, and readable format, where one of the circumstances set out in the Regulation applies.

- **Right to non-automated processing:** Data subjects shall have the right not to be subject to a decision affecting them, where that decision is based on automated processing of information, including profiling.

10. RECORD OF PROCESSING ACTIVITIES

Allfunds shall keep a record of the processing activities carried out within its organisation, the information to be included in this record being different when the Company acts as Data Controller or Data Processor.

In this regard, 'processing of personal data' means any process or technical operation, whether automated or not, that enables collection, recording, storage, preparation, alteration, consultation, use, cancellation, blocking or deletion of data, as well as transfers of data obtained from communications, consultations, combination and transfer of data that directly or indirectly identify or may directly or indirectly a natural person.

11. PRIVACY IMPACT ASSESSMENT

Processing of personal data is exposed to certain risks during the life cycle of the processing. These risks shall be identified, managed, and reduced to a reasonable level in order to protect to the rights and freedoms of natural persons.

The GDPR introduced the concept of Privacy Impact Assessment ('PIA'") as a new risk-analysis tool for safeguarding personal data. It specifically provides that where a type of processing by its nature, scope, context or purposes, and in particular if it uses new technologies, of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the Controller shall, prior to the processing, carry out an assessment of the processing operations' impact on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

It therefore sets out (i) the basis for preparing a PIA; (ii) the cases where such assessment should be carried out; (iii) the information to be provided; (iv) the involvement of the DPO; and (iv) other related questions.

However, due to the subjective nature of the need to carry out a PIA, Allfunds has a methodology in place that allows to perform a preliminary risk assessments to determinate whether a PIA is necessary. This ensures a more objective approach, setting out the minimum steps and the requirements to be considered in the assessment of whether the processing poses a high risk to the rights and freedoms of data subjects. However, supervisory authorities have established

indicative and non-restrictive lists of these types of processing operations that will require a data protection impact assessment, in addition to those expressly provided for by GDPR:

- Systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person;

- Processing on a large scale of special categories of personal data relating to criminal convictions and offences.

- Systematic monitoring of a publicly accessible area on a large scale.

12. NOTIFICATION OF SECURITY INCIDENTS

Allfunds, as Controller, shall report to the Supervisory Authority without undue delay and no later than 72 hours after having become aware of it, of any breach of which it becomes aware, unless such breach is unlikely to result in a risk to the rights and freedoms of data subject.

Furthermore, where the personal data security breach is likely to result in a high risk to the rights and freedoms of natural persons, the Controller shall notify the data subject concerned as soon as reasonably feasible and in close cooperation with the Supervisory Authority, unless one of the circumstances set out in the Regulation applies.

If the processing is carried out by Allfunds or by a third party as Processor, the latter shall notify the Controller of any personal data breaches of which it becomes aware. Subsequently, the Controller shall subsequently notify the Supervisory Authority of the breach, as it would of any other personal data security breach if required to do so in accordance with applicable law.

In addition to the above, where the Data Protection Office becomes aware of a serious or material breach of data protection, it shall document it and inform the senior management and/or Board of Directors (through the Risk and Audit Board Committee).

Allfunds has defined a Procedure for Management of Security Incidents which states:

(i) the methodology for identifying and notifying a security incident to the DPO and other relevant areas impacted by the incident (ie. IT Information Security and Risk Management),
(ii) the classification of incidents,
(iii) the severity's assessment in the risk to the rights and freedoms of Data Subjects,
(iv) the incidents record keeping, and
(v) the notification process to the supervisory authority and management bodies.

This procedure is available for all employees in the intranet.

13. PENALTIES

Breach of data protection obligations may give rise to administrative fines of up to EUR 20 million, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year.

The fines envisaged in the GDPR therefore affect the entire Company as a whole. Accordingly, full compliance with this data protection framework is of fundamental importance, as it represents the minimum data protection requirements that Allfunds shall comply with when processing personal data.

14. AWARENESS-RAISING AND TRAINING

All employees of Allfunds, especially those who process personal data in his/her daily activities, shall have appropriate training for performing their tasks. Furthermore, Allfunds shall also ensure that all Relevant Persons have the appropriate level of awareness of privacy, personal data protection and related good practices.

To this end, the Data Protection Office, in close collaboration with the Human Resources department and other interested departments, shall carry out recurrent training and awareness-raising activities in this area for Allfunds staff. Likewise, as already indicated above, this policy and the rest of the data protection regulatory body will be available to all Allfunds employees on the group intranet. All Relevant Persons concerned shall know and comply with the same.

15. MONITORING AND UPDATING

ALLFUNDS will regularly review its General Privacy Policy and update it whenever necessary to adapt it to any applicable regulatory amendments.

The Data Protection Office, within the Compliance Department, oversees coordinating such monitoring and review.