



General Data Protection Regulation (GDPR) Policy

History of Updates

	TYPE OF DOCUMENT	VERSION	DATE OF APPROVAL	APPROVED BY
1	Policy	V.1	28/12/2020	The Board of Directors
2		V.2	04812/2024	The Board of Directors

TABLE OF CONTENTS

1. Introduction.....	4
1.1 Definitions.....	4
1.2 The Management Company	6
1.3 Regulatory Framework.....	6
1.4 Purpose	6
1.5 Scope	6
1.6 Private Notice Guarantee	7
2. Roles and Responsibilities	7
2.1 Board of Directors	7
2.2 Executive Committee	7
2.3 GDPR Designation of the Data Protection Officer	7
2.4 Compliance Officer / Data Protection Officer	8
3. Processing of Personal Data	9
3.1 Data Subjects	9
3.2 Candidates' Privacy Notice	9
3.3 Purpose of Processing	9
3.4 Format of Record Keeping Personal Data	10
3.5 Processor	10
3.6 The Recipients of the Personal Data	10
3.7 Storage Period of Personal Data	11
3.8 Transmission of Personal Data to Countries outside the European Economic Area	11
3.9 Principles Relating to Processing of Personal Data	11
4. Obligations of NBG AM Luxembourg as Controller	12
4.1 Obligation to Inform.....	12
4.2 Data Protection Impact Assessment	12
4.3 Safeguarding the Rights of the Subject	13
4.4 Security of Processing	13
4.5 Information Systems Security.....	13
4.6 Record Register.....	14
4.7 Obligations Regarding the Development of Systems and New Business Processes	14
5. Policy review and update.....	15
6. Annexes.....	16
6.1 ANNEX 1 - CATEGORIES OF PERSONAL DATA	16
6.2 Annex 2 - List of Processing Operations for which a Data Protection Impact Assessment (DPIA) is required (National Commission for Data Protection).....	16

1. Introduction

1.1 Definitions

Term	Definition
Data Protection Officer (DPO)	Data Protection Officer is an individual or entity appointed by an organization to oversee and ensure compliance with data protection laws and regulations, particularly under the General Data Protection Regulation (GDPR). The primary role of a DPO is to act as a point of contact between the organization, data subjects, and supervisory authorities regarding data protection issues.
Data Protection Impact Assessment (DPIA)	<p>A Data Protection Impact Assessment (DPIA) is a systematic process used to identify, assess, and mitigate risks associated with data processing activities that may impact the privacy and data protection rights of individuals. It is a key component of the General Data Protection Regulation (GDPR), specifically outlined in Article 35.</p> <p>A DPIA is therefore not necessary for all processing operations and should only be applied to high risk processing operations, according to commonly recognised and accepted criteria.</p>
CSSF	The “Commission de Surveillance du Secteur Financier”, which is the public institution supervising the professionals and products of the financial sector in Luxembourg.
CNPD	“Commission Nationale pour la Protection des Données”, the lead supervisory authority for the protection of personal data in Luxembourg for the processing operations carried out by efa (any request from the CNIL should in principle go through the CNPD, except in exceptional cases).
Customer	The “Customer” means collectively any Investor and/or Nominee, including UBOs and any person authorized to act on their behalf that intends to invest or is investing to Distributors.
Investor	Natural person or legal person that subscribes in or acquires shares of an Investment Vehicle for which efa provides administration services.
Personal data	Any information relating to an identified or identifiable natural person (‘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, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
Special categories of data (Sensitive data)	Data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, welfare and sexual life, and participation in associations related to the above mentioned persons (as listed in Annex A to this Policy).
Processing	Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
Restriction of processing	The marking of stored personal data with the aim of limiting their processing in the future;

Filing system	Any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;
Controller	The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data;
Personal data breach	Any breach of security resulting in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

1.2 The Management Company

NBG Asset Management Luxembourg, S.A (also named "NBG AM Luxembourg") is a public limited company (Société Anonyme) organised under chapter 15 of the Luxembourg law of 17 December 2010 on undertakings for collective investment as amended from time to time (loi concernant les organismes de placement collectif) (the "2010 Law") which implemented into the Luxembourg law (i) the Directive 2009/65/EC of the Parliament and of the Council of 13 July 2009 on the coordination of laws, regulations and administrative provisions relating to UCITS, as amended from time to time (the "Directive 2009/65/EC") and (ii) the implementation measures of the Directive 2009/65/EC. NBG AM Luxembourg is a subsidiary of National Bank of Greece S.A. (NBG S.A.).

NBG AM Luxembourg is committed to conducting its business in accordance with applicable laws and regulations, and in a way which protects its reputation in the market. It is crucial that each employee shares in this commitment.

NBG AM Luxembourg as the Controller, recognizes and prioritizes the obligation to comply with applicable law with regard to the general protection of the individual from the processing of personal data.

NBG AM Luxembourg collects and manages specific information regarding Board members, employees, clients with which it maintains any form of business relationship, with whom it maintains a cooperative relationship, and with third parties in any relationship other than referred to above. This information, which contains personal data, will be managed in a lawful manner regardless of the means of collection or storage, ensuring compliance with applicable law and confidentiality.

1.3 Regulatory Framework

This Policy has been drawn up in line with the requirements of the existing legislative and regulatory framework for the processing of personal data, in particular taking into account:

- the Law of 1 August 2018 on the organisation of the Commission Nationale pour la Protection des Données ("CNPD") [the Luxembourg Data Protection Supervisory Authority] and the general data protection regime;
- Regulation (EU) 2016/679 of 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);
- Amended Act of 30 May 2005 ((data protection and electronic communications - Coordinated text from 10.08.2011) concerning the specific provisions for protection of the individual in respect of the processing of personal data in the electronic communications sector, and amending Articles 88-2 and 88-4 of the Code of Criminal Procedure;
- Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector, as amended by Directive 2009/136/EC.

1.4 Purpose

With this policy NBG AM Luxembourg seeks to:

- Comply with the applicable legal and regulatory framework for the management of personal data;
- Strengthen the information governance system and ensure the management of information containing personal data, in accordance with the provisions of existing legislation;
- Ensure the protection of personal data in the context of the implementation of its systemic functions;
- A clear definition of the principles and rules governing the processing of personal data brought to its attention during a business or other cooperation relationship, with a view to protecting the rights and fundamental freedoms of natural persons, in particular privacy;
- Awareness and guidance of personnel to avoid acts that could lead to administrative, civil or criminal sanctions (fine/revocation of license/destruction of file/interruption of processing and destruction of the relevant data - compensation - periodic penalty payment/imprisonment respectively) for breach of the provisions of national and European data protection law;
- The protection of its reputation and credibility, both as a NBG AM Luxembourg and as a member of the National Bank of Greece Group. (NBG Group).

1.5 Scope

This Policy:

- Commits NBG AM Luxembourg as it establishes the basic principles governing the processing of personal data;
- Applies to all members of the Board, Conducting Officers, employees of NBG AM Luxembourg, and in general to all persons employed by NBG AM Luxembourg, either by contract of employment or otherwise (e.g. Management consultants, any Staff of cooperating companies with NBG AM Luxembourg, etc.);
- Binds all third parties providing services for or in the name and on behalf of NBG AM Luxembourg (including partners, intermediaries, and any other persons with whom NBG AM Luxembourg cooperates in outsourcing or other types of agreements);
- Covers all the activities of NBG AM Luxembourg, including all the operations carried out by NBG AM Luxembourg, consultant or third party acting on behalf of or in cooperation with NBG AM Luxembourg;
- Covers all forms of processing carried out to serve NBG AM Luxembourg's business and relating to the keeping, either of physical or of electronic records.

1.6 Private Notice Guarantee

The Company complies with all applicable laws and regulations relating to processing of personal data and privacy. As GDPR requires Controller provides detailed specific information to Data Subject regardless of whether the information was collected directly from data subjects or from elsewhere. The information must provide through appropriate privacy notices.

NBG Asset Management collects personal data directly from data subjects, including for human resources or employment purposes (not limited on that) the Company must provide the data subject (or/and keep a copy of Current policy in the Company's site, with all the information required by the GDPR including the identity of the Controller and how and why Company will use, process, disclose, protect and retain that Personal Data through private notice.

2. Roles and Responsibilities

2.1 Board of Directors

The Board of Directors of NBG AM Luxembourg is responsible for the adoption and the approval of this Policy and its periodic review, upon the recommendation of the Compliance Officer / Data Protection Officer.

The Board of Directors is responsible for the adoption of this Policy, adjusted as appropriate to the nature, scope and complexity of the Company's activities.

2.2 Executive Committee

The Executive Committee is responsible to establish the necessary procedures for the proper implementation of the Policy.

The Executive Committee ensures that the staff are trained in matters relating to the processing of personal data.

The Executive Committee evaluates the adequacy and effectiveness of this policy and is responsible for its review, in regularly, after the Compliance Officer / Data Protection Officer's suggestion, in accordance with any changes in the legal and regulatory framework and taking into account NBG AM Luxembourg's strategic plans.

2.3 GDPR Designation of the Data Protection Officer

1. The controller and the processor will designate a Data Protection Officer in any case where:

- the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
- the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
- the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 Regulation (EU) 2016/679 or personal data relating to criminal convictions and offences referred to in Article 10 Regulation (EU) 2016/679.

2. A group of undertakings may appoint a single Data Protection Officer provided that a Data Protection Officer is easily accessible from each establishment.
3. Where the controller or the processor is a public authority or body, a single Data Protection Officer may be designated for several such authorities or bodies, taking account of their organizational structure and size.
4. the controller or processor or associations and other bodies representing categories of controllers or processors may or, where required by Union or Member State law will, designate a Data Protection Officer. The Data Protection Officer may act for such associations and other bodies representing controllers or processors.
5. The Data Protection Officer will be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39 of Regulation (EU) 2016/679.
6. The Data Protection Officer may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract.
7. The controller or the processor will publish the contact details of the Data Protection Officer and communicate them to the supervisory authority.

2.4 Compliance Officer / Data Protection Officer

The primary role of the Compliance Officer / Data Protection Officer is to ensure that NBG AM Luxembourg processes the personal data of its staff, Providers or any other individuals in compliance with the applicable data protection rules.

The Compliance Officer / Data Protection Officer has at least the following tasks:

- to assist the Board and the Executive Committee – acting as Controller, whenever required, with the formulation, consistent implementation and review of this Policy;
- to act as the contact point for the supervisory authority on issues relating to processing, and to consult, where appropriate, with regard to any other matter.
- to monitor the legal framework for the processing of personal data and arrange for the submission of proposals to the Controller, in order to harmonize the policy with regulatory developments;
- to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;
- to be responsible for coordinating all necessary actions to complete the risk measurement of the processing of personal data, and for informing the Controller of its results;
- to monitor NBG AM Luxembourg's compliance with national and European data protection provisions and with the NBG AM Luxembourg's or processor policies in relation to the protection of personal data, carrying out audits on at least an annual basis;
- to monitor and implement instructions from the European Commission on the implementation of the provisions of the General Regulation on the protection of personal data;
- to keep the list of databases and the list of personal data breaches;
- to provide advice where requested as regards the Data Protection Impact Assessment and monitor its performance;
- to ensure a timely and effective response to requests from data subjects;
- to develop training material for personal data protection training in accordance with the regulatory and legislative framework and for the provision of guidance on practical issues and on how issues are managed by the staff of NBG AM Luxembourg processing personal data;
- to provide guidance on all aspects of handling personal data issues;
- to cooperate with the supervisory authority;

The controller and the processor shall ensure that the Data Protection Officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

The Controller and processor shall support the Data Protection Officer in performing the tasks referred above by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.

The Controller and processor shall ensure that the Data Protection Officer does not receive any instructions regarding the exercise of those tasks. He or she shall not be dismissed or penalised by the controller or the processor for performing his tasks. The data protection officer shall directly report to the highest management level of the controller or the processor.

Data subjects may contact the Data Protection Officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this Regulation.

The Data Protection Officer is bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law.

The Data Protection Officer may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.

3. Processing of Personal Data

NBG AM Luxembourg, as the Controller, processes personal data, which it maintains in its records. In particular, the following apply:

3.1 Data Subjects

Subjects of the personal data processed by NBG AM Luxembourg and kept in a file are:

- Potential clients¹;
- Clients (unit-holders in a managed NBG AM Luxembourg UCITS)²;
- The members of the Board of Directors of NBG AM Luxembourg;
- The staff of NBG AM Luxembourg (through a dependent or independent relationship) and candidates;
- The partners with NBG AM Luxembourg.

In particular with regard to the protection of children's data:

NBG AM Luxembourg recognizes the need to protect children's data as defined by the existing statutory framework. NBG AM Luxembourg does not deal directly with children and its products and services are not intended for direct use by children. NBG AM Luxembourg only deals with the holder of parental responsibility over the children.

3.2 Candidates' Privacy Notice

NBG AM Luxembourg will collect and process candidate's personal information and will be responsible for complying with applicable data protection laws (Regulation (EU) 2016/679 ("GDPR")). NBG AM Luxembourg respects applicants' privacy and will treat those personal information as confidential.

This information will be obtained from candidates' application file and/or documents requested during the recruitment process. Data will be stored in different places, including in candidate's application record, in the NBG AM Luxembourg management systems and email system, all of which are in Luxembourg. The NBG AM Luxembourg does not use the information candidate provided to make any automated decisions that might affect applicant.

3.3 Purpose of Processing

The processing of personal data by NBG AM Luxembourg covers a wide range of operations performed on personal data, including by manual or automated means. It includes the collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of personal data.

The processing includes:

- staff management and payroll administration;
- access to/consultation of a contacts database containing personal data;

¹ The company distributes its funds based on a Distribution model. The Distributors and Transfer Agent handle the personal data of (i) Customers and (ii) Investors.

² The company distributes its funds based on a Distribution model. The Distributors and Transfer Agent handle the personal data of (i) Customers and (ii) Investors

- shredding documents containing personal data.

3.4 Format of Record Keeping Personal Data

NBG AM Luxembourg holds personal data processed in writing and / or in electronic form.

3.5 Processor

NBG AM Luxembourg appoints service providers to process personal data on its behalf. NBG AM Luxembourg uses only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing meet the requirements of EU /national data protection laws and ensure the protection of the rights of the data subject.

NBG AM Luxembourg appoints the processor in the form of a binding written agreement that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of NBG AM Luxembourg and stipulate, in particular, that the processor must:

- only act on NBG AM Luxembourg's documented instructions;
- impose confidentiality obligations on all personnel who process the relevant data;
- ensure the security of the personal data that it processes;
- abide by the rules regarding appointment of sub-processors;
- implement measures to assist the controller in complying with the rights of data subjects;
- assist NBG AM Luxembourg in obtaining approval from Compliance Officer / Data Protection Officer where required;
- at NBG AM Luxembourg's election, either return or destroy the personal data at the end of the relationship (except as required by EU or national law); and
- Provides NBG AM Luxembourg with all information necessary to demonstrate compliance with the GDPR.

3.6 The Recipients of the Personal Data

Recipients of the personal data, which NBG AM Luxembourg is required or entitled to communicate under a legislative or regulatory provision or a judicial decision or under the lawful functioning of the transactional and contractual relationship of the subjects with it, may be third parties in relation to NBG AM Luxembourg, natural or legal persons, public authorities, services or other entities, such as:

- a) The National Bank of Greece and Companies of the National Bank Group;
- b) The Ethniki Hellenic General Insurance SA'
- c) Any credit institution perform the function of depositary/sub - depositary of the NBG AM Luxembourg's managed UCITS, the intermediaries for the allocation of units of NBG AM Luxembourg's UCITS, as well as third parties-providers to whom NBG AM Luxembourg has, under an agreement, delegated the exercise of functions under the UCITS management and providing customer portfolio management;
- d) Insurance Institutions, Public Organizations, Chamber of commerce and Public Authorities or bodies;
- e) Supervisory Authorities, courts and other judicial authorities, Independent and other Authorities at national and European level;
- f) Auditors and audit firms.

Please note that NBG AM Luxembourg will also provide more specific information on any transition of data of subjects to the above recipients, if provided for by the applicable legislation.

NBG AM Luxembourg may disclose the personal data of the subjects to the competent Supervisory, Independent, Police, Judicial and Public Authorities, where required by the applicable legal and regulatory framework, on a regular or exceptional basis, if requested or if it is required to report such data without prior specific information.

Please note that where NBG AM Luxembourg entrusts the processing of personal data to the third parties who act on behalf of NBG AM Luxembourg, they must fully comply with NBG AM Luxembourg's instructions. This compliance is ensured through specific provisions in the relevant outsourcing contractual and compliance procedures.

3.7 Storage Period of Personal Data

The period for which the personal data are stored is limited to a strict minimum in order to ensure that the personal data are not kept longer than necessary, time limits are established by NBG AM Luxembourg for erasure or for a periodic review.

Personal data 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. Personal data may be stored for longer periods in accordance with the statutory framework in force for the period provided for by the end of the business relationship or for as long as is necessary for the establishment, exercise or defense of legal claims of NBG AM Luxembourg.

NBG AM Luxembourg carries out personal data related to criminal convictions and offences. For that reasons maintains a record of processing activities under its responsibility. In addition, NBG AM Luxembourg maintains a record of all categories of processing activities carried out on behalf of a controller.

That record will contain:

- a) the name and contact details of the Controller and where applies of joint controller and controllers' representative, and Data Protection Officer;
- b) the purposes of the processing and description of categories of both data subjects and personal data;
- c) the categories of recipients to whom personal data shared or disclosed, including those in third countries of International organizations;
- d) the envisaged time limits for erasure of the different categories of data;
- e) a general description of the technical and organizational security measures (*if applicable*).

The records will be kept in writing, including in electronic form. NBG AM Luxembourg will make the record available to the supervisory authorities upon request.

3.8 Transmission of Personal Data to Countries outside the European Economic Area

Any transfer of personal data to countries outside the European Economic Area may take place only if those countries provide an adequate level of protection of personal data. Where a third country outside the European Economic Area does not provide an adequate level of personal data protection, personal data may be transmitted to that country only if having entered into standard contractual clauses in accordance with the procedures provided for by the European Commission for the transfer of personal data to sub-contractors established in third countries or any other appropriate guarantees as defined in article 46 of the GDPR.

In the case mentioned above, NBG AM Luxembourg will ensure the safe processing of the personal data transmitted.

3.9 Principles Relating to Processing of Personal Data

NBG AM Luxembourg, as the controller, ensures that the personal data are:

- a) Processed lawfully, fairly and in a transparent manner in relation to any data subject;
- b) Collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes;
- c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- d) Accurate and, where necessary, kept up to date, with every reasonable step being taken to ensure that any inaccurate personal data are erased or rectified without delay;
- e) 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; and
- f) Processed in accordance with the rights of data subjects.

4. Obligations of NBG AM Luxembourg as Controller

4.1 Obligation to Inform

Where personal data relating to a data subject are collected from the data subject, NBG AM Luxembourg, as controller, will, at the time when personal data are obtained, provide the data subject with all of the following information:

- a) its identity and the contact details of its representative;
- b) the contact details of the Compliance Officer / Data Protection Officer;
- c) the purposes of the processing for which the personal data are intended;
- d) the legitimate interest of NBG AM Luxembourg in the processing of personal data, where applicable;
- e) the recipients or categories of recipients of the personal data;
- f) whether their personal data will be transferred to a recipient outside the EU;

In addition, NBG AM Luxembourg will, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing;

- a) the period for which the personal data will be stored;
- b) the existence of the right to request from NBG AM Luxembourg access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
- a) the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
- c) the right to lodge a complaint with the Commission Nationale pour la Protection des Données ("CNPD");
- d) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;
- e) the existence of automated decision-making, including profiling.

Where data collection and processing does not require the consent of the subject, the information will be provided in the most appropriate way, in order to ensure uninterrupted and sufficient information to the subject.

For example, information may be provided:

- with a clear warning visible label in the transaction area;
- with printed material available;
- with an indication in accounts, invoices or other supporting documents, if a trading relationship is existed;
- with a clear indication in the questionnaire, application form, information document, etc., if the subject is required to complete it;
- with a specific, clear and visible label on the website, where the collection is done via the internet.

Please note that the obligation to provide information may be waived in whole or in part for reasons expressly provided for in European and national legislation on the protection of personal data (such as for reasons of national security or for the prevention, investigation, detection or prosecution of criminal offenses).

4.2 Data Protection Impact Assessment

As NBG Asset Management outsources distribution services to third-party companies and only handles employee data, the overall risk associated with personal data processing is low. However, a Data Protection Impact Assessment (DPIA) will be conducted when processing activities might still pose a high risk to the rights and freedoms of individuals, particularly when new technologies are involved or when sensitive data is processed.

DPIA Criteria

A DPIA will be performed if any of the following conditions are met:

- Processing involves sensitive or highly personal data.

- New technological or organizational solutions are applied.
- Processing could hinder employees' ability to exercise their rights.

If two or more of these criteria are met, the Data Protection Officer (DPO) will carry out a DPIA. In cases where the need for a DPIA is unclear, the DPO will assess the situation to determine if one is necessary.

The DPO will maintain records of all DPIAs conducted. If a DPIA identifies high risks that cannot be mitigated, the Supervisory Authority will be consulted.

4.3 Safeguarding the Rights of the Subject

Accordance with the relevant provisions of the applicable statutory framework, NBG AM Luxembourg informs the data subjects of their rights and ensures to develop the internal procedures to respond promptly and effectively to the data subjects in the exercise of their rights. NBG AM Luxembourg has designated the Compliance Officer / Data Protection Officer to handle data subjects' request for the exercise of their rights.

4.4 Security of Processing

Regarding the processing to be carried out by the processor on behalf of NBG AM Luxembourg, when entrusting a processor with processing activities, NBG AM Luxembourg uses only processors providing sufficient guarantees, in particular in terms of expert knowledge, reliability and resources, to implement technical and organisational measures which will meet the requirements of the security of processing.

In addition, NBG AM Luxembourg has appropriate applications based on high security standards for the protection of personal data, while the required checks are regularly scheduled.

NBG AM Luxembourg maintains records of any authorized access to its information systems. These include the name and surname of the user, the workstation from which he had access to the computer system, the date and time of access, the personal data he had access to, and the type of access with the actions taken during the processing of the information of personal data, authorization file for each access, file for any unauthorized access, and file for automatic rejection from the computer system.

If the carrying-out of processing by a processor should be governed by a contract or other legal act under Union or Member State law, binding the processor to NBG AM Luxembourg, setting out the subject-matter and duration of the processing, the nature and purposes of the processing, the type of personal data and categories of data subjects, taking into account the specific tasks and responsibilities of the processor in the context of the processing to be carried out and the risk to the rights and freedoms of the data subject. In order to ensure the confidentiality required provided that the processing is performed only on instructions and on behalf of the Company and other obligations regarding confidentiality and security of processing accordingly charged and the third service provider.

In addition, NBG AM Luxembourg takes appropriate organizational and technical measures to ensure data security and to protect them from breaches such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed which may in particular lead to physical, material or non-material damage. Those measures ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected.

The processor notifies the Compliance Officer / Data Protection Officer without undue delay after becoming aware of a personal data breach. The Compliance Officer / Data Protection Officer systematically records infringements and assess the reasons for such breaches. In addition, the Compliance Officer / Data Protection Officer takes the necessary measures to restore security and prevent recurrence of breaches.

The Compliance Officer / Data Protection Officer notifies the personal data breach to the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it. In addition, the Compliance Officer / Data Protection Officer communicates to the data subject a personal data breach if necessary, accordance with the regulatory framework. Details of the required actions are specified in NBG AM Luxembourg's Data Breach Management Process.

4.5 Information Systems Security

In order to ensure the confidentiality of all information stored in its information systems, NBG AM Luxembourg has adopted an Information Technology Security Policy, which includes a reference to NBG AM Luxembourg's implementation and the IT Group Security Policy Framework.

These are available internally to NBG AM Luxembourg's staff, listing the terms and conditions to be observed in order to:

- protect data transmitted through the data networks used by NBG AM Luxembourg;
- control the access of users to the Company's information systems and ensure the protection of the information, that these systems manage;
- identify in a timely manner and prevent, as far as possible, incidents of security breach of NBG AM Luxembourg's IT systems;
- apply the encryption methods required in the handling of confidential and confidential information or data in order to ensure the integrity, confidentiality and availability of such information.

4.6 Record Register

NBG AM Luxembourg maintains a record of processing activities, which includes all information required under the regulatory framework.

4.7 Obligations Regarding the Development of Systems and New Business Processes

The protection of personal data is an integral part of NBG AM Luxembourg's technological development and organizational structure. In this context, NBG AM Luxembourg is already designing new products, services and applications, taking appropriate technical and organizational measures to ensure, by definition, the systematic and secure management of personal data life cycle from the collection and processing to delete them.

In particular, NBG AM Luxembourg ensures the follows:

- Data processing systems collect only the personal data that is strictly necessary to fulfil the purpose for which they were collected;
- Where data anonymization does not interfere with the purpose of the data processing, personal data becomes anonymous so that the data subject can no longer be identified;
- Where personal data cannot be made anonymous, appropriate security measures will be taken depending on the nature of the data, such as falsification, encryption or restriction of access;
- Access to personal data is permitted only to persons who are required to have access to them in order to perform their duties;
- Systematic quality control of personal data is part of the data lifecycle management to ensure high data quality. Data processing systems are adequately protected against unauthorized access through technical and organizational measures.

NBG AM Luxembourg informs the data subjects of their rights under the applicable legal and regulatory framework. In particular, those rights include:

Right to Inform	The NBG AM Luxembourg informs the data subject of any information concerning the processing of its data in a summary, comprehensible and easily accessible form, using clear and simple wording.
Right of access	The data subject will, upon request, obtain from the controller confirmation of to whether or not the personal data concerning him or her are processed and, if so, the data subject may exercise his or her right of access to the data in question.
Right to Rectification	The data subject has the right to obtain from the NBG AM Luxembourg without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject has the right to have incomplete personal data completed, including by means of providing a supplementary statement.
Right to erasure ('right to be forgotten')	The data subject has the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller will have the obligation to erase personal data without undue delay under specified conditions.
Right to restriction of processing	The data subject has the right to obtain from the NBG AM Luxembourg restriction of processing under specified conditions.
Right to Object	The data subject has the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her. The NBG AM Luxembourg will no longer process the personal

Right related to automated decision-making, including profiling	<p>data unless the NBG AM Luxembourg demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defense of legal claims.</p> <p>The data subject has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.</p>
Right to data portability	<p>The data subject has the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided.</p>

The employees of NBG AM Luxembourg are required to respect any request for data subject concerning the exercise of their rights and, if necessary, to consult the Compliance Officer / Data Protection Officer. More information on the management of data subject's related requests for the exercise of their rights can be found in NBG AM Luxembourg's Data Subject Manage Request Process.

5. Policy review and update

The Compliance Officer / Data Protection Officer updates this policy whenever needed, in order to take into account changes in the legal and regulatory environment applicable to NBG Asset Management Luxembourg's activities. Any change will be reviewed by the Executive Committee and approved by the Board of Directors. Such approval will be documented in written minutes of the Board of Directors and kept available at the registered office of NBG AM Luxembourg.

6. Annexes

6.1 ANNEX 1 - CATEGORIES OF PERSONAL DATA

Group A: PERSONAL DATA (NON-SENSITIVE)

The following personal data is considered 'non-sensitive':

- (i) Identification;
- (ii) Demographic;
- (iii) Family conditions;
- (iv) Education;
- (v) Economic situation;
- (vi) Work;
- (vii) Electronic communications data.

Group B: SPECIFIC CATEGORIES OF DATA (SENSITIVE DATA)

The following personal data is considered 'sensitive' and is subject to specific processing conditions:

- (i) Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs;
- (ii) Trade-union membership;
- (iii) Genetic data, biometric data processed solely to identify a human being;
- (iv) Health-related data;
- (v) Data concerning a person's sex life or sexual orientation.

Group C: PERSONAL DATA RELATING TO CRIMINAL OFFENCES

The following personal data is considered:

- (i) Data related criminal convictions and offences;
- (ii) Data related security measures.

6.2 Annex 2 - List of Processing Operations for which a Data Protection Impact Assessment (DPIA) is required (National Commission for Data Protection)

- 1) Processing activities that rely on genetic data as defined under GDPR article 4 (13) in conjunction with at least one other criteria from the article 29 working party guidelines (WP248 rev. 01), except for healthcare professionals when providing healthcare services;
- 2) Processing activities that include biometric data as defined under GDPR article 4(14) and have as a purpose identification of data subjects in conjunction with at least one other criteria from the article 29 working party guidelines (WP248 rev. 01);
- 3) Processing activities involving the combination, matching or comparison of personal data collected from processing activities having different purposes (from the same or different data controllers) – provided that they produce legal effects concerning the natural person or similarly significantly affects the natural person;
- 4) Processing activities that consist of or include regular and systematic monitoring of employee activities - provided that they might produce legal effects concerning the employees or similarly significantly affects them;
- 5) Processing activities on files that might contain personal data of the whole national population provided that such a DPIA has not already been carried out as part of a general impact assessment in the context of the adoption of that legal basis;
- 6) Processing activities that have a scientific, historical research purpose or a statistical purpose as required in Article 65 of the law of August 1st, 2018 (*Loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et mise en oeuvre du règlement (UE) 2016/679 du parlement européen et du Conseil du 27 avril 2016*) ;
- 7) Processing activities that consist in systematic tracking of natural persons position;

- 8) Processing activities based on indirect collection of personal data when it is not possible / feasible to guarantee the right of information in conjunction with at least one other criteria from the article 29 working party guidelines (*WP248 rev. 01*).