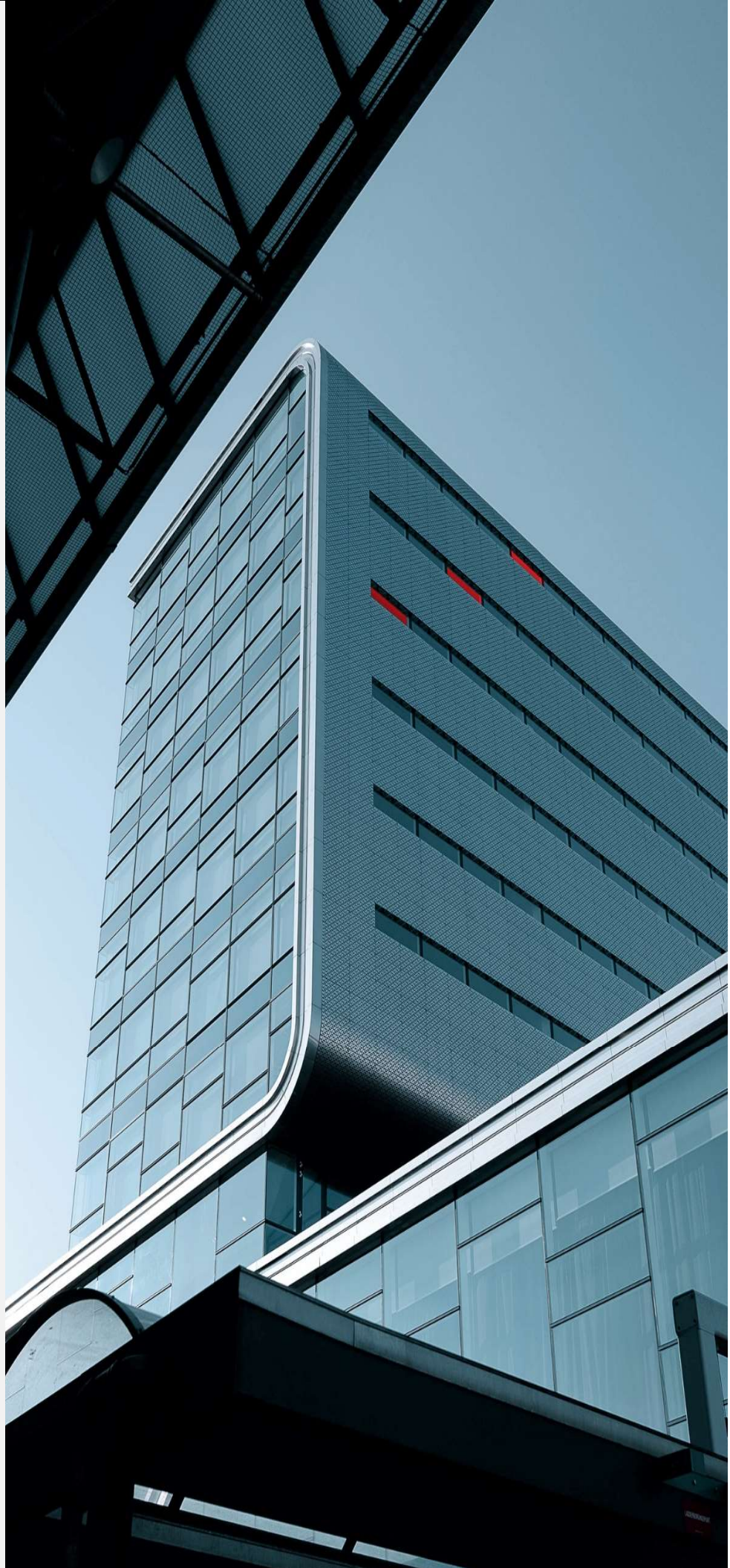
GDPR Policy

SAM LUX
Compliance

February 2023



1. INTRODUCTION

1.1 Santander Asset Management Luxembourg S.A. ("**SAM Luxembourg**") recognizes the importance of respecting the privacy of its clients, investors, employees, and other parties with whom it does business. SAM Luxembourg protects and respects the personal integrity of these latter and strives to establish the necessary awareness of the importance of data protection and privacy issues. SAM Luxembourg aims to reduce the risks of violations and ensure that all Personal Data is maintained in a lawful, fair and transparent way as well as ensure governance and accountability to facilitate data protection compliance. SAM Luxembourg in the performance of its business activities seeks to comply with relevant and applicable privacy laws and regulations.

1.2 This GDPR policy ("**Policy**") is intended to serve as a framework document setting down basic principles on the handling of Personal Data and applies to everyone at SAM Luxembourg – all employees, including managers and executive officers, as well as the board of directors (which are included in the term "**employees**") for the purpose of this Policy. This Policy describes how SAM Luxembourg processes Personal Data when carrying out its function as management company. This Policy also lays down certain provisions regarding confidentiality which complements other internal rules of SAM Luxembourg.

1.3 The purpose of this Policy is to secure that SAM Luxembourg:

a) observes professional secrecy with respect to all customer relations and comply with relevant confidentiality regimes; and

b) respects the right to privacy and as prescribed by relevant laws, circulars and regulations, upholds Personal Data protection, when processing Personal Data.

1.4 All employees are obliged to ensure that they are aware of and have understood the content of the Policy and their related rights and responsibilities. If you have any questions related to the Policy, please contact the Compliance Officer or the DPO. Training will be provided to all staff to enable them to carry out their obligations within this Policy.

2. KEY TERMS

"**CNPD**"	means the Commission Nationale pour la Protection des Données.
"**Compliance Officer**"	means the compliance officer of SAM Luxembourg.
"**Controller**"	means an entity that determines the purposes and means of the processing. In some cases, there can be more than one Controller. When

	SAM Luxembourg processes Personal Data, it might do so on its own initiative, determining the purposes and means of the processing. In these types of situations, SAM Luxembourg will be acting as a Controller. For example, SAM Luxembourg is a Controller when it collects, stores, and uses information about its employees in order to pay them a salary or to know whom to contact in an emergency. Similarly, SAM Luxembourg is generally a Controller when it maintains a database of representatives of service providers of SAM Luxembourg.
"**Controller to Controller**"	means when two companies are sharing Personal Data and are determining the purpose and means of the processing separately for its respective processing of Personal Data, they are both considered Controllers and not Joint Controllers. This might be the case when a company sells its customer database to another company, which will use the Personal Data for marketing purposes.
"**Data Protection Authority**"	means the authority/authorities in each given national jurisdiction charged with the oversight and enforcement of the GDPR.
"**Data Subject**"	means the identified or identifiable person to whom specific Personal Data relates.
"**DPO**"	means the data protection officer of SAM Luxembourg.
"**EEA**"	means the European Economic Area – this refers to the countries of the European Union as well as Iceland, Lichtenstein, and Norway.
"**EU**"	means the European Union.
"**Joint Controllers**"	means the situation when two companies are working together, either jointly or separately, and are mutually determining the purposes and means of processing, the companies are considered joint Controllers.

"**GDPR**"	means the 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.
"**Investors**"	means investors, ultimate beneficial owners, directors, authorised representatives, or contact persons of investors of the investment funds managed by SAM Luxembourg.
"**Personal Data**"	means any information relating to an identified or identifiable natural person (i.e. a Data Subject – see above). A person can be identified by their name, ID number, location, an online identifier, or even aspects of their physical, physiological, genetic, mental, economic, cultural, or social identity.
"**Personal Data Breach**"	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.
"**Processing**"	means any kind of activity carried out on Personal Data such as collecting, organising, storing, using, altering, combining, disclosing, restricting, or erasing.
"**Processor**"	means a person or entity that processes Personal Data on behalf of the Controller. While the Controller determines the purpose and nature of how the Personal Data is processed, the processor merely carries out the activity. Processors have their own obligations under data protection regulations, such as ensuring appropriate technical and organisational measures to ensure security. Examples of processors are IT service providers, such as cloud service providers.
"**Profiling**"	means any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating

	to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
"**Sensitive Personal Data**"	means special categories of Personal Data, namely genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, data concerning a person's sex life or sexual orientation, as well as data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership.

3. SCOPE OF GDPR

3.1 GDPR applies to Personal Data, which means information directly or indirectly relating to a living natural person. Data relating to a legal person is not generally subject to GDPR.

3.2 GDPR applies to:

(i) Companies located in the EU/EEA even if the processing of the data takes place outside the EU/EEA; and

(ii) Companies located outside the EU/EEA when the companies market goods/services to individuals in the EU/EEA or engage in monitoring activities of individuals' behaviour in the EU/EEA (such as profiling activities).

3.3 GDPR does not apply to information, which is completely anonymous, i.e. information which cannot be related back to an identifiable individual. It does, however, apply to information which has undergone so-called pseudonymisation, i.e. information which can be linked to an individual with the use of another set of information (such as a "**key**"). Personal data which has undergone encryption, and no longer can be related to a natural person without the encryption key, is considered to be pseudonymised.

3.4 Companies which do not comply with the provisions of GDPR can be exposed to financial and reputational risks and criminal sanctions. This may very well have a significant impact on the entire Santander entities. In addition, any individual who has suffered damage (which can be non-financial) has the right to receive compensation from the non-compliant company.

4. PERSONAL DATA PROTECTION

4.1 Roles

4.1.1 SAM Luxembourg shall produce and maintain necessary instructions and procedures to comply with GDPR and the laws, circulars and regulations in the context of GDPR.

4.1.2 In relation to Personal Data concerning the Investors, the investment funds managed by SAM Luxembourg and SAM Luxembourg will act as Joint Controllers. In case that the investment fund is a common fund, SAM Luxembourg will act as sole Controller.

4.1.3 When SAM Luxembourg on behalf of the Joint Controllers commissions to another natural or legal person within the EEA, to process Personal Data on behalf of the Joint Controllers, a contract (a personal data processing agreement) shall be entered into with the third party that is acting as Processor. The contract shall be binding on the Processor and shall set out: (a) the subject-matter and duration of the processing; (b) the nature and purpose of the processing; (c) the type of Personal Data and categories of Data Subjects; (d) the obligations and rights of the Joint Controllers; (e) state that the Processor may process Personal Data solely in accordance with the Joint Controllers' instructions and according to applicable data protection regulations; (f) require the Processor to implement and maintain appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the GDPR and to ensure confidentiality and security of processing; and (g) shall stipulate the requirements imposed on the Processor described in article 28.3 of GDPR.

4.1.4 SAM Luxembourg will be the Controller in relation to data processing relating to its employees.

4.2 Data Protection Officer

4.2.1 Appointment of the DPO

The board of directors of SAM Luxembourg shall appoint a person to serve as DPO when its core activities 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 when its core activities consist of processing on a large scale of special categories of data.

4.2.2 Requirements of the DPO

In case a DPO is appointed, he/she shall be a person with good knowledge on internal and external rules on data privacy.

The DPO should also have a good understanding of the processing operations carried out, as well as the information systems, and data security and data protection needs of SAM Luxembourg. Further, the person appointed as DPO may only be entrusted with other tasks and duties that do not give rise to conflicts of interests with his/her role as DPO.

The DPO shall be easily accessible and shall be able to communicate with Data Subjects and the CNPD in the language(s) used by the Luxembourg supervisory authorities and the Data Subjects.

The contact details (a postal address, a dedicated telephone number, and a dedicated e-mail address) of the DPO shall be published and communicated to the relevant supervisory authorities.

4.2.3 Position of the DPO

In case a DPO is appointed, SAM Luxembourg shall ensure that he/she is involved, properly and in a timely manner, in all issues which relate to the protection of Personal Data.

Further SAM Luxembourg shall support the DPO in performing the DPO´s tasks providing resources necessary to carry out those tasks and access to Personal Data and processing operations.

The DPO shall be given sufficient time to fulfil his/her duties as DPO and be given the opportunity to stay up to date with regard to regulatory developments within data privacy.

SAM Luxembourg remains responsible for compliance with GDPR. Responsibility in this domain cannot be delegated.

The DPO shall be given the opportunity to perform his/her duties and tasks in an independent manner as described in article 38.3 of GDPR. No instructions can be given to a DPO regarding how to exercise his/her tasks as DPO. He/She shall have the right to contact and seek advice from the supervisory authority and may not be dismissed or penalised for performing his or her tasks as DPO. The DPO shall report to the board of directors of SAM Luxembourg.

In case a DPO is appointed, he/she shall be bound by secrecy and confidentiality concerning the performance of his or her tasks, in accordance with Member State law.

4.2.4 Tasks of the DPO

In case a DPO is appointed, he/she shall act as contact point for and cooperate with the CNPD.

The DPO shall provide advice in relation to and monitor compliance with the GDPR, other external and internal rules on Personal Data protection. As part of the duty to monitor compliance, the DPO may, e.g. collect information to identify processing activities, analyse and check the compliance of processing activities and inform, advice and issue recommendations.

The DPO shall inform and advise SAM Luxembourg and its employees who carry out processing of their obligations pursuant to the GDPR and to Member State data protection provisions.

The DPO shall be involved, properly and in a timely manner, in all issues which relate to the protection of Personal Data including but not limited to when data protection impact assessments are carried out and if a Personal Data Breach has occurred.

The DPO shall carry out his/her work in a risk-based manner. This means having due regard to the risk associated with the processing operations, taking into account the nature, scope, context and purposes of processing when planning and carrying out his or her tasks.

4.3 Personal Data Processing principles

4.3.1 General

Personal Data may only be processed lawfully (on the basis of the legal grounds set out in section 5 of this Policy), fairly and in a transparent manner. Further, SAM Luxembourg shall be able to demonstrate compliance with the principles for processing stipulated in this Policy.

4.3.2 Data fairness

Personal Data may only be processed in a way that is fair. This means Personal Data must not be processed in a way that is unduly detrimental, unexpected or misleading to the Data Subjects concerned.

4.3.3 Purpose limitation

Personal Data may only be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Legitimate purposes as regards employee related Personal Data are e.g. staff administration (appointments or removals, pay, discipline, pension plans, work management or other personnel matters in relation to staff) and as regards Investors related Personal Data e.g. central administration, registrar and transfer agency, domiciliation and paying agency services, market analysis, business and method development, risk and compliance management.

4.3.4 Retention and deletion of Personal Data

Personal Data may be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data are processed.

4.3.5 Data minimisation

Whenever and to the extent possible, SAM Luxembourg anonymises the Personal Data which SAM Luxembourg holds about the Data Subjects.

4.3.6 Data accuracy and proportionality

Personal Data must be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that Personal Data that are inaccurate having regard to the purposes for which they are processed are

erased or rectified without delay. Furthermore, Personal Data must be adequate, relevant, and limited in relation to the purposes for which they are collected and/or further processed. Also, Personal Data shall only be processed in a manner that ensures appropriate security including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage using appropriate technical or organizational measures.

4.3.7 Integrity and confidentiality

SAM Luxembourg will ensure appropriate security of the Personal Data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

5. LEGAL GROUNDS FOR PROCESSING OF PERSONAL DATA

5.1 One of the principles of GDPR and this Policy is that the processing of Personal Data must be lawful. This means that it has to be based on one of the legal grounds specified in GDPR. In practice, there are four primary legal grounds, which are relevant for SAM Luxembourg and establish legitimate reasons for processing of Personal Data.

(i) ***Performance of contract***. If it is necessary for the fulfilment of a contract to which the Data Subject is a party.

(ii) ***Legitimate interest***. The legitimate interest of SAM Luxembourg to process Personal Data of an individual must be balanced against the individual´s fundamental rights to protection of his/her Personal Data. In cases where the individual is an employee, an Investor or a business contact, it can be reasonably expected by the individual that SAM Luxembourg will process Personal Data and that may constitute a legitimate interest. The processing of Personal Data for preventing fraud may also be a legitimate interest.

(iii) ***Legal obligation***. If it is necessary in order to comply with a legal obligation, for example if SAM Luxembourg as an employer has a legal obligation to file tax income information to tax authorities.

(iv) ***Consent***. If an individual has given consent to SAM Luxembourg for the processing of his/her Personal Data that constitutes a legal ground. The consent shall be distinct, phrased in clear and plain language, be given freely and must not contain any unfair terms. An individual can withdraw his or her consent at any time and shall be informed of this right when giving the consent. In relation to Personal Data of the Investors, consent will not be the legal basis for processing. However, consent will be used for candidates who have applied for a position in SAM Luxembourg.

5.2 SAM Luxembourg must always ensure that the legal ground for processing Personal Data is identified and documented for each purpose prior to the processing.

5.3 SAM Luxembourg will process Personal Data on the legal basis that most closely reflects the true nature of the relationship with the Data Subject and the purpose of the processing.

6. TRANSFERS OF DATA BETWEEN SANTANDER ENTITIES

6.1 Santander entities may process Personal Data for the purposes indicated in this Policy. Any processing carried out by any of the Santander entities is subject to the terms of this Policy and only the Personal Data which is necessary to provide the services requested by the Investors or the employees is processed by these entities.

7. CATEGORIES OF PERSONAL DATA THAT SHALL BE GIVEN SPECIAL PROTECTION

7.1 In accordance with the provisions of GDPR, the processing of Sensitive Personal Data and Personal Data relating to criminal offences and/or convictions is subject to greater restrictions.

This is detailed below.

7.2 Sensitive Personal Data

7.2.1 SAM Luxembourg may only process Sensitive Personal Data if at least one of the following conditions applies:

(i) ***Consent***. SAM Luxembourg has obtained clear, explicit consent from the Data Subject to their Personal Data being processed for the specific purpose(s) for which it is being processed. Please note that a Data Subject may withdraw his or her consent with immediate effect.

(ii) ***Employment law***. SAM Luxembourg needs to use the Personal Data to enact rights or obligations it has under employment law, social security law, or a collective bargaining agreement.

(iii) ***Personal data already made public***. The Personal Data was already visibly made public by the Data Subject.

(iv) ***Legal claims***. SAM Luxembourg needs to process the Personal Data to carry out legal claims.

(v) ***Other***. Under local regulation, there may be other permitted reasons for processing Sensitive Personal Data, such as for statistical purposes. If you consider it necessary for SAM Luxembourg to process Sensitive Personal Data for a particular purpose and none of the conditions listed above apply, please contact the DPO / Compliance Officer for further guidance.

7.3 Personal data relating to criminal convictions and offences

7.3.1 SAM Luxembourg will not process Personal Data relating to criminal convictions and offences except in relation to its business activities and as may be requested by the CSSF like for instance criminal records from the

directors, conducting officers, compliance officer, liquidators (if any) of SAM Luxembourg and in certain cases from the shareholders of SAM Luxembourg.

7.3.2 Processing of Personal Data relating to criminal convictions and offences, or related security measures based on article 6(1) shall be carried out in compliance with the Luxembourg law of 23 July 2016 amending inter alia the law of 29 March 2013 relating to the organisation of the criminal records.

8. TRANSPARENCY AND INFORMATION

8.1 In order to ensure fair and transparent processing SAM Luxembourg shall, if possible, well in advance, provide the Data Subject with all the information necessary to protect the privacy of the individual. The information will be provided in the "**Data Privacy Notice**" via SAM Luxembourg's website. Such information must be provided in a concise, transparent, intelligible, and easily accessible form, using clear and plain language.

8.2 When Personal Data is collected directly from a Data Subject, SAM Luxembourg must ensure that the Data Subject is provided with the following information:

(i) ***Name and contact details***. The name and contact details of SAM Luxembourg, which will be acting as data Controller as well as contact details of the function with responsibility for data protection and privacy and if a DPO is appointed contact details of the DPO.

(ii) ***Purpose.*** The purpose for which the Data Subject's Personal Data is processed and on the basis of wat legal ground as described in section 5. If the processing is carried out to fulfil a legitimate interest, then the interest must also be specified.

(iii) ***Recipients.*** Any recipients, or categories of recipients, with whom SAM Luxembourg will share the Personal Data.

8.3 To ensure fair and transparent processing of the Personal Data, the Data Subject must also be informed of any of the following insofar as necessary.

(i) ***Contractual or legal necessity*****.** Whether providing the Personal Data is necessary under law or in order to enter into/fulfil a contract, and the potential consequences of not providing the Personal Data.

(ii) ***Storage time*****.** Information on how long the Personal Data will be stored for. If it is not possible to provide an exact retention period, information should be provided on how the length of storage time will be determined.

(iii) ***Data subject rights*****.** The Data Subjects rights, e.g. to request access to their Personal Data, to request its erasure, rectification or restriction, to object to its processing, and to lodge a complaint with the CNPD.

8.4 The following situations do not take place when SAM Luxembourg processes Personal Data, should the following situations change in the future the Data Privacy Notice shall disclose the following:

(i) ***Use of automated decision making*.** Personal Data processed by SAM Luxembourg is as of today not subject to automated decision-making. If this situation changes in the future, the Data Privacy Notice shall describe whether the Personal Data will be subject to automated decision-making and necessary information on the process and its possible impact on the Data Subject; and

(ii) ***Profiling and direct marketing.*** Personal Data processed by SAM Luxembourg is as of today not subject to direct marketing or profiling. If this situation changes in the future, the Data Privacy Notice shall provide the necessary information on the process and its possible impact on the Data Subject.

8.5 When collecting Personal Data about a Data Subject from another source than the Data Subject, SAM Luxembourg should make sure that the Data Subject is kept informed. If possible (without seriously disproportionate effort relative to the Personal Data concerned), SAM Luxembourg must provide the Data Subject with information as is listed above, as well as the following additional information:

(i) ***Nature of the collected Personal Data*.** The categories of Personal Data that have been collected; and

(ii) ***Source of the collected Personal Data.*** If necessary to ensure that the Personal Data is processed in a fair and transparent manner, from which source the Personal Data originates.

9. RIGHTS OF THE INDIVIDUAL

9.1 To protect the rights and freedoms of individuals with regard to processing of Personal Data, it is required that the data is processed lawfully and in a transparent manner. In order for individuals to verify the accuracy and lawfulness of the processing of Personal Data, SAM Luxembourg must ensure that individuals can exercise their rights in relation to such processing.

9.2 The GDPR contains multiple rights of Data Subjects which aim to ensure that individuals are provided with information concerning when and how their Personal Data is processed. Thus, the individuals have the right to:

- have access to the Personal Data and be provided with a copy of the Personal Data being processed. The right of access of the Data Subject to his/her AML file can be restricted or delayed by virtue of article 6(10) of the Law of the 13 February 2018, and in accordance with the restrictions foreseen by article 23 of GDPR;

- have the Personal Data corrected, erased or limited, except that Personal Data will not be erased to the extent that processing is necessary for compliance with a legal obligation which requires

processing by Member State law to which SAM Luxembourg is subject or for the establishment, exercise or defence of legal claims. SAM Luxembourg shall communicate any rectification or erasure of Personal Data or restriction of processing carried out in accordance with this paragraph to each recipient to whom the Personal Data have been disclosed, unless this proves impossible or involves disproportionate effort. SAM Luxembourg shall inform the Data Subject about those recipients if the Data Subject requests it;

- object to the processing of Personal Data, when processing is based on consent or the Personal Data is used for direct marketing; and

- have the Personal Data transferred to another Controller upon request (data portability).

9.3 In order for SAM Luxembourg to demonstrate compliance with GDPR and the individuals' rights, SAM Luxembourg must know how to handle and administrate all types of requests from individuals whose Personal Data is being processed. This section 9 describes the rights of the individuals and how different requests should be handled in practice.

9.4 Important considerations when handling requests from individuals include knowledge of the scope of the different rights, how the requested information should be provided and what it should contain and within what timeframe the requests should be handled.

9.5 SAM Luxembourg shall provide information on action taken on a request under this section 9.5 and in any event within one (1) month of receipt of the request. The period may be extended by two (2) further months considering the complexity and number of requests. In case of such extension, the Data Subject shall be informed of the delay and the reasons therefore within one month of receipt of the request.

9.6 General information concerning requests from individuals

- SAM Luxembourg may not refuse to act on a request when an individual is exercising his/her rights, unless SAM Luxembourg can demonstrate that it is not possible to identify the Data Subject. If SAM Luxembourg has reasonable doubts concerning the identity of the individual, one may request additional information necessary for identifying the individual.

- After receiving the request SAM Luxembourg should provide information to the individual on the action taken without undue delay and in any event within one (1) month of the receipt of the request.

- If SAM Luxembourg does not take action on the request, the individual should without undue delay but within one (1) month of the request be informed about the reasons for not doing so and

about the possibility to lodge a complaint with a supervisory authority and seeking a judicial remedy.

- Make sure that no Personal Data is handed out to third parties (e.g. individuals asking for other individuals' Personal Data) and that secrecy laws do not limit the right to handle out certain Personal Data (e.g. regulations concerning trade secrets).

9.7 Copy of the Personal Data undergoing process

- In accordance with GDPR, Data Subjects have the right to request a copy of the Personal Data undergoing processing by SAM Luxembourg. This right can be exercised at reasonable intervals. To facilitate to respond to such requests, do not process Personal Data longer than is necessary.

- If an individual requests a copy of the Personal Data being processed, it is not enough to only provide information on what categories of Personal Data that is being processed. It may therefore be possible to give out a compilation of the Personal Data yet including the specific Personal Data that is being processed.

- If SAM Luxembourg processes a large amount of Personal Data of the individual, SAM Luxembourg may ask the individual to specify what information or which processing the request refers to.

- If the request is conducted digitally, the copy could preferably also be provided in a digital manner.

- If possible, SAM Luxembourg should provide remote access to the systems where the data is processed, which gives the Data Subject direct access to his or her Personal Data.

- Apart from providing the specific Personal Data being processed the individual should upon request be provided with the following information:

    (i) the purposes of the processing and the categories of Personal Data being processed;

    (ii) the recipients or categories of recipient to whom the Personal Data have been or will be disclosed and in case in the future Personal Data is transferred outside EEA, the recipients in third countries (countries outside the EU/EEA) or international organisations;

    (iii) the period for which the Personal Data will be stored, or, if not possible the criteria used to decide it;

    (iv) the rights of the individual (e.g. right to object, request erasure, restriction and correction of the Personal Data);

(v) the right to lodge a complaint with a supervisory authority;

(vi) from where the Personal Data has been collected if it is not collected by SAM Luxembourg; and

(vii) if the processing is based on an automated decision-making, including profiling and the logic involved in such decision-making and what consequences it caused for the individual when using such type of processing.

- The copies should be provided free of charge, unless requests are manifestly unfounded (e.g. if requests are repeated many times) or excessive (e.g. asking for a large amount of information from a long time period), SAM Luxembourg may charge a reasonable fee.

- SAM Luxembourg can deny the individuals' requests of obtaining a copy if it would adversely affect the rights and freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software in connection with remote access. However, SAM Luxembourg should still provide the Personal Data that is possible to hand out without causing consequences for other individuals.

9.8 SAM Luxembourg shall keep a register of Data Subject's request.

9.9 Data portability

- In accordance with the provisions of GDPR, the individuals have upon request the right to be provided with the Personal Data being processed in a machine-readable format and have the right to have the Personal Data transmitted to another data Controller. A machine-readable format includes all formats that easily can be processed by a computer, e.g. word-, PDF-, HTLM- files, xml, or other comparable format.

- The right to data portability may only be exercised if:

  (i) the processing is based on the performance of a contract, which is the case in relation to for example employees; or

  (ii) when the processing is based on consent, which is the case in relation to processing of for example pictures, and if its processed by automated means (i.e. not manually).

- The request does not need to be fulfilled:

  (i) if it is not technically feasible, e.g. if a fundamental technical adaption of the system is needed. Even if it is not possible to transmit the data to another Controller, the individual has the right to receive his/her Personal Data in a structured machine-readable format; or

(ii) if the Personal Data that is being requested to be transferred is processed based on other legal grounds than consent or performance of a contract, such as legitimate interest.

9.10 The right to erasure, correction, restriction and objection

- Individuals have the right to object to and request correction, limitation and erasure of the Personal Data being processed if they believe that the Personal Data is incorrect, misleading or otherwise not processed in accordance with applicable law. The actions should be taken without undue delay.

- When changing/deleting data in accordance with individuals' requests, SAM Luxembourg must ensure that the actions are taken in all systems and sources where the Personal Data is stated, e.g. intranet, employee folder, website, etc.

- When SAM Luxembourg has fulfilled a request regarding rectification, erasure or restriction of processing of Personal Data, SAM Luxembourg should if it does not imply a disproportionate burden and is practically possible, inform all individuals that have had access to the Personal Data about the action taken.

9.10.1 Erasure

- If the individual request erasure of the Personal Data SAM Luxembourg has to fulfil the request if:

  (i) the Personal Data is no longer needed to fulfil the purpose for which the Personal Data was being collected;

  (ii) the individual has withdrawn his/her consent, in case consent is the legal basis for processing;

  (iii) the Personal Data is processed only for purposes of direct marketing;

  (iv) SAM Luxembourg has processed the Personal Data unlawfully; or

  (v) SAM Luxembourg is obliged to do so in accordance with laws, circulars or regulations.

- If SAM Luxembourg has made the Personal Data publicly available, SAM Luxembourg must inform the ones responsible for erasing the Personal Data in the public source (e.g. website).

- When erasing Personal Data, one must make sure that the data is unreadable and impossible to re-create.

- SAM Luxembourg may deny a request of erasure if:

(i) the processing is necessary for exercising the right of freedom of expression and information;

(ii) it is needed to comply with a legal obligation; or

(iii) the processing is needed to exercise or defend a legal claim.

9.10.2 Correction

- The individuals have the right to request correction of Personal Data that is incomplete, incorrect or misleading. A correction measures can include making amendments to the already existing Personal Data.

9.10.3 Restriction

- Restriction of personal data means that SAM Luxembourg only may store the Personal Data but not process it further without the individual's consent, unless it is needed for the protection of the rights of another natural or legal person or it is needed for reasons of an important public interest.

- Methods for restricting Personal Data could include, among others, to temporarily remove the selected data to another processing system, making the selected Personal Data unavailable to users or temporarily removing published data from a website. In automated filing systems, the restriction of processing should in principle be ensured by technical means in such a manner that the Personal Data are not subject to further processing operations and cannot be changed. The fact that the processing of Personal Data is restricted should be clearly indicated in the system.

- If the individual makes a request for restriction of the Personal Data, SAM Luxembourg has to fulfil it:

  (i) if the accuracy of the Personal Data is contested by the individual;

  (ii) during the process of determining whether or not SAM Luxembourg as the Controller has an overriding interest where the processing is conducted in pursuance of a legitimate interest;

  (iii) if the processing is unlawful and the Data Subject opposes to erasure and wants the data to be retained; or

  (iv) if the Personal Data no longer is needed, but should be stored due to the exercise or defence of legal claims.

- If the processing is restricted in accordance with the individuals' request, SAM Luxembourg should inform the individual.

- Processing of Personal Data that has undergone a restriction, can only be processed by SAM Luxembourg:

  (i) if the individual has consented to processing in relation to exercise or defence of legal claims; or

  (ii) if the processing is needed for the protection of the rights of another natural or legal person; or

  (iii) if it is needed for reasons of an important public interest.

9.10.4 Objection

- If the individual objects to the processing of Personal Data, the objection is only valid when SAM Luxembourg has based its processing on a legitimate interest which is a legal ground used, e.g. when using recruitment systems that exclude candidates based on certain requirements.

- If an objection is valid, the general rule is that SAM Luxembourg has to stop processing Personal Data, unless SAM Luxembourg can show that they have compelling legitimate grounds for the processing that override the interests and rights of the individuals.

- SAM Luxembourg may deny a request of objection if:

  (i) the processing is based on the performance of a contract, such as in relation to most of the processing concerning employees or the Investors; and

  (ii) the processing is based on consent, such as in relation to the use of pictures.

- However, please note that other requests may be valid in relation to processing based on performance of a contract and consent, such as correction and restriction.

9.11 Automated individual decision-making, including profiling

- The individuals shall have the right not to be subject to a decision based solely on automated decision-making, including Profiling, which produces legal effects or similarly significantly affects the individual.

  - **Profiling** includes automated forms of processing; carried out on Personal Data; with the objective of evaluating personal aspects about a natural person. Simply assessing or classifying individuals based on characteristics such as age and height could be considered Profiling.

  - **Automated decision-making** entails the ability to make decisions by technological means without human involvement, which can include Profiling.

- **A legal effect** may be something that affects a person's legal status or their rights under a contract. For example, automated decisions that mean someone is denied a particular social benefit granted by law.

- **Significantly affects** the individuals entails that the data processing must be more than trivial, and must have the potential to significantly influence the circumstances or behaviour of the individuals concerned.

- **Appropriate safeguards** includes the provision of information to individuals, and also the obligation to provide the possibility of obtaining human intervention, express his/her point of view and to contest the decision.

10. RECORD OF PROCESSING OF PERSONAL DATA

10.1 SAM Luxembourg is legally required to maintain a record of all its data processing activities, regardless of if it is acting as Controller or processor.

10.2 The record shall include information on:

- The name and contact details of the Controller/Processor and the unit responsible for data processing or when applicable the DPO;

- The purposes of the processing;

- The categories of individuals concerned and Personal Data processed;

- The categories of processing carried out by SAM Luxembourg on behalf of a Controller (in case SAM Luxembourg is acting as Processor);

- The categories of recipients with whom the Personal Data may be shared;

- If applicable, information regarding cross-border data transfers (i.e. transfers of Personal Data outside the EU/EEA) and documentation of suitable safeguards;

- The applicable data retention periods; and

- A description of the security measures implemented to protect the Personal Data.

10.3 SAM Luxembourg must ensure that all processing activities are documented and that the record is up to date. If a DPO is appointed keeping the information in the record of Personal Data, up to date will be his/her responsibility.

11. CONTROLLER AND PROCESSOR

11.1 Responsibility

11.1.1 Each time SAM Luxembourg processes Personal Data, it will do so either as a Controller or as a Processor. In light of GDPR, SAM Luxembourg has direct obligations and may face direct enforcement and sanctions regardless of whether it is acting as Controller or Processor. However, SAM Luxembourg's responsibilities will differ depending on the role. Hence, it is important for SAM Luxembourg to identify when it acts as a Controller and as a Processor, respectively. This applies both externally and for intra-group scenarios.

11.2 Data Processor Agreements and Joint Controllers

11.2.1 GDPR requires that SAM Luxembourg, in the role as Controller, can guarantee that a data processor agreement is in place whenever any Personal Data is transferred to or processed by a different entity. This applies both to an external entity (such as an IT service provider or cloud service provider) or an internal entity (e.g. when Personal Data is transferred between entities within the Santander entities). The data processor agreement must stipulate terms regarding the processing of Personal Data conducted on behalf of SAM Luxembourg. Such terms include, amongst other things, instructions to the Processor and a specification of the respective responsibilities of the Controller and Processor.

11.2.2 Conversely, when SAM Luxembourg acts as a Processor instead of Controller and processes Personal Data on behalf of other companies, SAM Luxembourg must fulfil the obligations of the role as Processor as set out in GDPR and the data processor agreement.

11.2.3 In certain situations, SAM Luxembourg may be deemed to be a Joint Controller when processing Personal Data in collaboration with another company. Such a relationship should be governed in a transparent manner determining the respective Controller's responsibilities (similar to a data processor agreement). This is the case when processing Personal Data relating to the Investors, SAM Luxembourg and the investment funds act as Joint Controllers.

11.2.4 In other situations, SAM Luxembourg may also share Personal Data with another Controller that has its own purposes for the processing of Personal Data. If that is the case, both the Controllers need to enter into an agreement regulating their relationship and the sharing of Personal Data from Controller to Controller.

11.2.5 This section serves as a guideline to fulfil the requirements of GDPR and ensure the lawful processing of SAM Luxembourg's Personal Data when SAM Luxembourg conducts business with and receives services from third parties that involve the processing of Personal Data.

11.3 When to enter into a data processor agreement

11.3.1 In order to be able to determine if SAM Luxembourg shall enter into a data processor agreement, the following considerations should be made:

- Does the relationship with the external party (e.g. provision of service, correspondence, etc.) include a transfer of Personal Data (e.g. name, email address, identification number, picture, payment information, customer preferences, location data, information about health etc.)?

- Is SAM Luxembourg acting as a Controller, Processor or Joint Controller in the relevant context?

11.3.2 If the transfer includes Personal Data, and if:

- SAM Luxembourg is acting as a Controller, please be referred to section 11.4;

- SAM Luxembourg is acting as a Joint Controller together with another external party, please be referred to section 11.5;

- SAM Luxembourg is sharing Personal Data with or receiving Personal Data from another separate Controller, please be referred to section 11.6;

- SAM Luxembourg is acting as a Processor, please be referred to section 11.7;

- The external party is providing a data processor agreement, please be referred to section 11.8, and

- The Personal Data is transferred between SAM Luxembourg and a party located outside of the EU/EEA, further requirements apply, please be referred to section 11.9.

11.3.3 When using template agreements, please ensure that the templates are completed with accurate and relevant details about the parties, the Personal Data being processed and the agreement, project or activity that has triggered the need for the template agreement. Template agreements must include all the relevant requirements in GDPR and are designed to protect the interests of SAM Luxembourg, depending on whether it is acting as the Controller, the Processor or as Joint Controller.

11.4 When SAM Luxembourg acts as Controller

11.4.1 When SAM Luxembourg acts as Controller, SAM Luxembourg must ensure that there is a data processor agreement in place with the Processor. The data processor agreement shall, amongst other things, regulate the Processor's implementation of appropriate technical and organisational measures in order to guarantee that the Personal Data is processed in a secure manner. Additionally, when SAM Luxembourg is acting as a

Controller it is the responsibility of SAM Luxembourg to provide instructions to the Processor concerning how the processing should be conducted.

11.4.2 When SAM Luxembourg is acting as the Controller, SAM Luxembourg should make sure that a data processor agreement is entered into.

11.5 When SAM Luxembourg acts as Joint Controller

11.5.1 When SAM Luxembourg acts as a Controller together with another Controller and decides the purposes and means together with the other Controller, a joint data Controller agreement has to be entered into. The agreement shall, in a transparent manner, determine the respective responsibilities of both Controllers for compliance with the obligations under GDPR and especially in relation to:

- The exercising of the rights of the Data Subject, and
- The Controllers' respective duties to provide information to the Data Subject.

11.5.2 SAM Luxembourg acts as Joint Controller together with the investment funds in relation to Personal Data of the Investors.

11.5.3 The arrangement should be made available to the Data Subjects and irrespective of the arrangement between the Controllers, the individuals may exercise their rights in relation to any of the Controllers.

11.6 When Personal Data is shared with or received from another Controller

11.6.1 In some situations, SAM Luxembourg may collaborate with another party in connection with, for example, the provision of a service. In contrast to the situation where two Controllers are considered joint Controllers, as described in section 11.5, the Controllers are determining the purpose and means for the respective processing of Personal Data separately. Furthermore, it is of utmost importance not to confuse this situation with the situation where the external party acts as SAM Luxembourg's Processor.

11.6.2 Please note that if the conditions for the processing changes and entail that one of the Controllers processes Personal Data on behalf of the other Controller, a data processor agreement as described below in section 11.4 should be entered into.

11.7 When SAM Luxembourg acts as Processor

11.7.1 When SAM Luxembourg acts as a Processor it must ensure that it has implemented appropriate technical and organisational measures and that it will only process Personal Data in accordance with the instructions given by the Controller.

11.8 When the other party provides a data processor agreement

11.8.1 In some situations, the external party may have its own agreement, terms or clauses relating to processing of Personal Data that is wishes to utilise. For

example, when SAM Luxembourg uses a large (IT and cloud) service provider like Microsoft or Google, there may be limited scope for revision or negotiation of the terms.

11.8.2 The largest globally and internationally known (IT and cloud) service providers are likely to have established extensive terms and conditions in relation to the processing of Personal Data. Although such terms and conditions are expected to comply with GDPR and applicable data protection regulations, it is important that SAM Luxembourg ensures that the relationship with such suppliers is supported by a proper and reasonable data processor agreement in light of the requirements and obligations set out in GDPR. Especially when the Personal Data being processed is of a high volume or sensitive by nature. The Controller must not accept standardised agreements provided by large IT and cloud service providers (acting as processors) without conducting such assessment. It is the obligation of the Controller to give instructions to the processor in order to ensure lawful and relevant terms for the processing at hand, and not the other way around.

11.9 When Personal Data is transferred outside of the EU/EEA

11.9.1 Personal Data may only be transferred outside of the EU/EEA with adequate protection. In order to comply with this requirement, if need be, SAM Luxembourg must ensure that one of the following is applicable:

- ***Approved country***. Data transfers to the country have been approved by the EU Commission through an "adequacy decision". A list of currently approved countries can be found on the website of the European Commission; or

- ***Approved contract***. SAM Luxembourg can ensure adequate protection by including special language in its processor agreements called EU Model Contract Clauses.

11.9.2 Please note that there are some exceptions to this rule. Indeed, SAM Luxembourg may transfer Personal Data to a country outside the EU/EEA without an adequate standard of protection in the following circumstances:

(i) ***Explicit and informed consent***. The Data Subject has been informed of the associated risks of such a transfer without adequate protection or safeguards and nevertheless explicitly consents to the transfer;

(ii) ***Contract***. The transfer is necessary for fulfilling a contract with the Data Subject. This can also include preparatory steps that SAM Luxembourg might make prior to entering into the contract, if done at the Data Subject's request;

(iii) ***Legal Claims***. The transfer is necessary for the enactment of legal claims; or

(iv) ***One-off limited transfer for legitimate interests***. The transfer is a one-off transfer that:

- concerns a limited number of Data Subjects;

- is necessary for SAM Luxembourg to pursue a compelling legitimate interest which is not overridden by the rights or interests of the Data Subjects;

- was done after a careful assessment of the circumstances and with suitable safeguards, both of which are documented; and

- SAM Luxembourg informs the relevant Data Protection Authority of the transfer and also informs the Data Subject of the transfer and the legitimate interest being pursued.

12. OUTSOURCING AND CLOUD-BASED SERVICES

12.1 When SAM Luxembourg wants to outsource services to third parties (such as IT service providers and cloud service providers) involving the processing of Personal Data, this will trigger data protection considerations. Generally, the service providers will act as Processor and a written processor agreement need to be put in place.

13. COOKIES

13.1 Prior consent is required for the use of cookies unless the cookie is strictly necessary for the provision of a service to that user.

13.2 Personal Data will not be used for direct marketing which implies Profiling.

14. DATA PROTECTION BY DESIGN AND BY DEFAULT

14.1 General guideline

The principles of data protection by design and by default should be taken into account when SAM Luxembourg is developing, designing, selecting and using applications, services and products that include processing of Personal Data. These principles should be implemented both at the time of the determination of the means for processing and at the time of the processing itself.

As an example, it would be relevant to consider data protection by design and by default when SAM Luxembourg builds new IT systems for storing or accessing Personal Data, develops policies or strategies that have data protection implications, initiates data sharing or uses data for new purposes.

Designing projects, processes, products or systems with data protection by design and by default in mind at the outset has several benefits, including:

- The possibility to identify potential problems at an early stage;

- The awareness of privacy and data protection across the organisation;

- The likeliness to meet the obligations of applicable data protection regulations, including GDPR, increases and equally, the likelihood of breaches is decreased; and

- Projects, processes, products or systems are less likely to be privacy intrusive and have a negative impact on individuals.

14.2 Data protection by design

14.2.1 What is data protection by design?

Data protection by design is a concept and approach to system engineering that takes data protection into account throughout the engineering process.

14.2.2 What does data protection by design entail in practice for SAM Luxembourg?

Data protection by design measures could consist, among other things, of:

(a) **Minimising the processing of Personal Data**. For example, only process Personal Data that is necessary for the purpose, limit the Personal Data to information that only indirectly can lead to identification of an individual, limit the Personal Data to information that is less sensitive, do not by default include personal identification numbers in databases or registries unless specific local legislation demands it;

(b) **Pseudonymise Personal Data as soon as possible**. For example if Personal Data must be collected, pseudonymise the information as soon as possible, or use pseudonyms at the outset;

(c) **Transparency with regard to the functions and processing of Personal Data**. For example, include functions that enable individuals to obtain copies of the Personal Data that is processed regarding them, include functions that enable individuals to gain access to the Personal Data, use a log to trace all third parties that have gained access to the Personal Data; and

(d) **Protect the Personal Data by adding technical and organisational security measures**. For example, the pseudonymisation and encryption of Personal Data, implement functions for password requirements for access, use encrypted information when communicating over the internet, through databases or mobile devices, implement routines and information regarding the security to all system users, use secure backup methods.

Different sorts of Personal Data may require different levels of security measures. When deciding which technical and organisational measures to implement in protection of the rights of the individual(s), SAM Luxembourg should consider the state of the art, the cost of implementation of such measures and the nature, scope, context and purposes of the processing in relation to the risk embedded in such processing. For example, Sensitive

Personal Data such as information about ethnic origin, political opinions, religion, health data, among others, requires a higher level of protection than not sensitive information.

In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed.

14.3 Data protection by default

14.3.1 What is data protection by default?

Data protection by default means that the strictest privacy settings automatically apply once a customer acquires a new product or service. In other words, no manual change to the privacy settings should be required on the part of the user. There is also a temporal element to this principle, as Personal Data must by default only be kept for the amount of time necessary to provide the product or service.

14.3.2 What does data protection by default entail in practice for SAM Luxembourg?

SAM Luxembourg shall implement appropriate technical and organisational measures for ensuring that, by default, only Personal Data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of Personal Data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default Personal Data are not made accessible without the individual's intervention to an indefinite number of individuals.

15. DATA PROTECTON IMPACT ASSESSMENT[1]

15.1 Where a type of processing (e.g. when new technologies will be deployed) is likely to result in a high degree of risk for individuals, SAM Luxembourg must conduct a data protection impact assessment. Conducting a data protection impact assessment is an important compliance tool and will allow SAM

[1] Please note that there is no need to carry out a data protection impact assessment:

- Where the processing is not "likely to result in a high risk to the rights and freedoms of natural persons" (art. 35(1) GDPR);
- When the nature, scope, context and purposes of the processing are very similar to the processing for which DPIAs have been carried out. Results of DPIAs for similar processing can be used (art. 35(1) GDPR);
- When the processing operations have been checked by a supervisory authority before May 2018 and the processing has not changed since (see III.C and also page 13 of WP29 Guidelines on DPIAs);
- Where a processing operation has a legal basis in EU or Member State law and has stated that an initial DPIA does not have to be carried out, where the law regulates the specific processing operation and where a DPIA has already been carried out as part of the establishment of that legal basis (art. 35(10) GDPR). This is the case of processing for AML KYC reasons; and
- Where the processing is included on the optional list established by the CNPD or processing operations for which no DPIA is required (art. 35(5) GDPR).

Luxembourg to address and mitigate data protection risks. SAM Luxembourg shall consider whether or not to carry out a data protection impact assessment, if a DPO has been appointed same should be consulted and the advice of the DPO and the decisions taken by SAM Luxembourg should be recorded in minutes.

15.2 If it is decided to carry out a data protection impact assessment. It should be reviewed and re-assessed on an on-going basis. SAM Luxembourg will be responsible for carrying it out and the DPO should monitor the performance of the same.

16. DATA ANALYTICS AND PROFILING

16.1 Data analytics enables SAM Luxembourg to make connections, identify patterns, predict behaviour and personalise interactions, and it makes it possible to discover additional information about for example employees and consumers that would not be known from examining the underlying data. However, when discovering and using this type of Personal Data, for consumer or employee profiling, etc., data protection aspects must be considered, including the application of the basic principles in GDPR and techniques, such as data protection by design (please be referred to section 14).

16.2 An individual may only be subject to a decision by SAM Luxembourg based solely on automated processing if the individual has given his or her explicit consent to the processing or if it is necessary for entering into or performance of a contract between SAM Luxembourg and the individual. This implies that for decisions made on the basis of data analytics and Profiling, SAM Luxembourg needs to ensure that the individual has consented to such processing or that it is necessary for entering into or performance of a contract with the individual. Automated decision could for example be an automatic refusal of an online credit application or e-recruiting practices without human intervention.

17. DATA SECURITY

17.1 General guideline: appropriate technical and organisational security measures

17.1.1 SAM Luxembourg must always have appropriate technical and organisational measures in place to ensure the ongoing confidentiality, integrity, availability, and resilience of its processing activities. When implementing such technical and organisational measures, state of the art technologies, the costs of implementation and the nature, scope, context and purposes of processing shall be taken into consideration. Depending on the nature of the processing these measures may include.

(i) Anonymisation or pseudonymisation and encryption of Personal Data;

(ii) The ability to ensure confidentiality, integrity, availability and resilience of processing systems and services;

(iii) The ability to maintain and restore the availability and access to Personal Data; and

(iv) A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures.

17.2 Communication

17.2.1 Communication is an important management tool and an instrument for communicating SAM Luxembourg's objectives and operations. A consistent and reliable communication is necessary, whilst regulatory requirements and employee integrity must be safeguarded. When Personal Data is processed through different communication channels, e.g. e-mail, letter, fax or IT-systems, there is always an impending risk that other than the intended recipient may get access to the Personal Data. Consequently, it is of utmost importance that appropriate procedures that ensure the safety of the Personal Data are considered when such data is communicated

17.2.2 One must ensure that the right recipient is specified when Personal Data is communicated. Please note that there is always an extended risk when Personal Data is processed through email because it is difficult to ensure that only the intended recipient will access the message. It may be difficult to secure the identity of a recipient solely on the basis of an email address. Names and email addresses may be filled in automatically or from mailing lists that can cause the email or letter to be accidentally sent to the wrong recipient or to considerably more recipients than the sender intended. One should send letters or hardcopies to a named individual by special delivery.

17.2.3 One must always ensure that the Personal Data has arrived at the right recipient. This is especially important when communicating confidential Personal Data, Sensitive Personal Data or Personal Data which may be deemed to require special protection (e.g. personal identity number or Personal Data relating to criminal convictions and offences, as well as data of children and vulnerable persons, or images of individuals). If you become aware that Personal Data has been communicated to the wrong recipient and this may constitute a Personal Data Breach, please follow SAM Luxembourg's procedure in case of Personal Data Breach.

17.2.4 Ensure that adequate security measures are in place, such as tools commonly used to protect information, e.g. firewalls and anti-virus software. There may be security shortcomings in email systems and copies of received and sent emails containing Personal Data may be saved on several servers, locally on an individual user's computer or in an individual user's mailbox, which is especially critical if the email account is accessible via an open network or synchronized with mobile devices (such as laptops and mobile phones).

17.2.5 Avoid leaving open emails on the computer screen. If the computer is in a place where it potentially can be accessed by other individuals, use a password-activated screen saver so that Personal Data is not visible to other individuals. It is important to limit the exposure of Personal Data on paper or hard copies as well. Paper or hard copies containing Personal Data should

be handled with care and never be left without supervision or handed out to a group of unspecified recipients.

17.3 Sensitive Personal Data

17.3.1 If confidential Personal Data, Sensitive Personal Data or Personal Data which may be deemed to require special protection (e.g. personal identity number or Personal Data relating to criminal convictions and offences, as well as data of children and vulnerable persons, or images of individuals) is communicated or shared, extended security measures and actions such as encryption or sending by courier are often required. The required level of security should be based on the following considerations.

(i) Which risks for integrity the processing entails;

(ii) How sensitive the processed Personal Data is;

(iii) What technical measures are at hand to protect the Personal Data; and

(iv) The costs for implementing such technical measures.

17.3.2 Confidential Personal Data, Sensitive Personal Data or Personal Data which may be deemed to require special protection (e.g. personal identity number or Personal Data relating to criminal convictions and offences, as well as data of children and vulnerable persons, or images of individuals) preferably be emailed in password protected files using a service that ensures encryption. The password should then be sent to the individual by separate email or communicated verbally.

18. PERSONAL DATA BREACHES

18.1.1 A Personal Data Breach is a breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data that SAM Luxembourg transmits, stores or processes (e.g. a hacker attack). In case of a Personal Data Breach considered as high risk to the rights and freedoms of natural persons, SAM Luxembourg must report the breach to the CNPD and in some cases to the relevant Data Protection Authority, and in some circumstances to the concerned individual, in accordance with applicable regulatory requirements.

18.1.2 The Compliance Officer or in case there is a DPO the latter will analyse if a breach is considered as high risk to the rights and freedoms of natural persons and if so ascertained he/she will report it to the Conducting Officers and board of directors of SAM Luxembourg, following their decision, a preliminary information notice should be sent to CNPD (within 72 hours) informing them that a breach has occurred and that SAM Luxembourg is investigating further.

18.1.3 Same procedure will apply in case an employee becomes aware of a Personal Data Breach. The employee will report it to the Compliance Officer, and the Compliance Officer will report to the DPO. if any and the latter will analyse it and in case it is considered as high risk by the board of directors

notify the CNPD and in some cases also notify the Data Subjects. Where feasible, the preliminary report of Personal Data Breach must be reported to the relevant Data Protection Authority no later than 72 hours after detecting the Personal Data Breach.

18.1.4 The notification of a Personal Data Breach to the supervisory authority shall at least include:

- a description of the nature of the Personal Data Breach including where possible, the categories and approximate number of individuals concerned and the categories and the approximate number of personal records concerned;
- the name and contact details of the unit responsible for data protection or other contact point where information can be obtained;
- a description of the likely consequences of the Personal Data Breach; and
- a description of the measures taken or proposed to be taken by SAM Luxembourg to address the Personal Data Breach, including where appropriate, measures to mitigate its possible adverse effects.

18.1.5 The communication to the individuals, to implement when the Personal Data Breach likely to result in a high risk to the right and freedoms of the individuals, shall include:

- a description, in clear and plain language, of the nature of the Personal Data Breach;
- the name and contact details of the unit responsible for data protection or other contact point where information can be obtained;
- a description of the likely consequences of the Personal Data Breach; and
- a description of the measures taken or proposed to be taken by SAM Luxembourg to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

18.1.6 If an employee suspects there has been a Personal Data Breach, he/she should notify the department responsible for data protection or the Compliance Officer, if any, immediately. SAM Luxembourg follows a policy of non-retaliation, and no employee will be subject to retaliatory action for reporting, in good faith, a suspected violation of this Policy.

18.1.7 SAM Luxembourg shall keep a register of Personal Data Breaches.

19. TRAINING

19.1 SAM Luxembourg shall provide appropriate training to its employees, as needed, on the Policy and applicable data protection regulations. At a minimum the training shall:

(i) Provide sufficient knowledge of the Policy and applicable data protection regulations;

(ii) Raise awareness of situations in which a director or the Compliance Officer;

(iii) Should or must be consulted and how to do so; and

(iv) Be provided to all new employees.

20. COMPLIANCE

20.1 Failure to follow this Policy may subject an employee to disciplinary action, up to and including termination of the employment contract.