Extract of our RAM's Personal data protection policy

JANUARY 2019

Contents **Page**

1 Document objectives

This policy (the "Policy") has been drawn up in accordance with the Article 24, paragraph 2, of Regulation (EU) 2016/679 (the "GDPR", or the "Regulation") repealing Directive 95/46/EC on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

The Policy defines:

(i) The general principles applicable to RAM, in its capacity as controller of personal data and the general measures adopted in order to comply with such principles;

(ii) The adoption of the applicable principles, measures, duties and responsibilities of RAM Group[1] (RAM Active Investments S.A.,RAM Active Investments (Europe) S.A. and their branches located in the European Union).

(iii) The Group Data Protection Team revises the Policy at least annually and assesses any amendments that need to be made. Every substantial alteration to the document must be approved by the Boards of Directors of RAM, the Compliance Committee, and whenever needed by any other relevant Committee.

Any amendments deriving from i) organizational changes, ii) issuance of or amendments to second-level regulations (e.g. by the Luxembourg personal data privacy authority) are made, at the Compliance Committee and DPT's proposals, with reporting to the Boards of Directors for approval;

The Policy cames into force on 25 May 2018 and was revised on 23 January 2019.

2 General principles and measures on personal data protection

The Policy sets out the principal measures identified by RAM to ensure compliance with the general principles contained in the GDPR, with reference in particular to (i) Lawfulness of processing, (ii) Rights of data subjects; (iii) Record of processing activities and data protection impact assessment (so called DPIA); (iv) Processing security; and (v) Management of data breach events. In this connection RAM:

(i) Adopts suitable processes, instruments and controls to allow full compliance with the general principles for processing personal data;

(ii) Guarantees adequate reporting flows from and to the relevant Committees and Teams;

[1] Including whenever it is relevant, all SICAVS promoted/managed by RAM with domicile in 14 boulevard Royal L-2449 Luxembourg

(iii) Ensures staff awareness of data protection key aspects and provide staff training to ensure compliance with the applicable regulations by any person performing personal data processing activities within the company organization under the authority of the controller.

The processing of personal data for the various categories of parties involved performed by RAM is based on the following principles:

- **Lawfulness, fairness and transparency**: personal data are collected and processed in a way that is lawful, fair and transparent in relation to the data subject;
- **Purpose limitation**: personal data are collected and processed for given, explicit, legitimate purposes;
- **Minimization of data**: personal data are adequate, relevant and limited to what is strictly necessary for the purposes for which they are processed;
- **Accuracy**: personal data are accurate and, where necessary, kept up-to-date and every step must be adopted to ensure that personal data that are inaccurate, are erased or rectified in a timely manner.;
- **Storage limitation**: personal data are retained for a period of time which does not exceed the achievement of the purposes for which they were collected;
- **Integrity and confidentiality**: personal data are processed in such a way as to safeguard their security, through adoption of the appropriate technical and organizational measures;
- **Privacy by design and privacy by default**: personal data protection issues must be taken into consideration right from the phases of design, implementation and configuration of all technologies used for the processing activities. RAM must by default process only such data as is necessary to achieve the purposes of the processing;
- **Accountability**: personal data are processed in accordance with the principles set out above and compliance with these principles is to be adequately documented.

2.1. Lawfulness of processing

Personal data may be processed within RAM solely on the basis of at least one of the following conditions:

- **Contract** to which the data subject is a party;
- **Legal obligation** to which RAM is subject;
- Safeguarding **vital or public interests**;
- Explicit **consent** granted by the data subject;
- Pursuit of a **legitimate interest** by RAM.

2.1.1. Request for consent

Where personal data is processed on the basis of the data subject consent, such consent is collected in the form of a written statement, or in certain cases for which the risk profile is lower, in verbal form which is then documented in writing. If the data subject's consent is given in the context of a written declaration which also concerns other matters the request for consent shall be presented in a manner which is clearly distinguishable from other matters, in an intelligible and easily accessible form, using clear and plain language. Such consent

may be withdrawn at any time and its withdrawal shall not compromise the lawfulness of processing based on consent before its withdrawal.

2.1.2. Legitimate interest

In some cases (e.g. direct marketing), the procedures instituted by RAM must stipulate that the personal data may be processed for the purpose of RAM pursuing a legitimate interest.

2.1.3. Transfer of data

RAM Active Investments (Europe) S.A.: personal data may be transferred to another country (not forming part of the European Union) or an international organization without specific authorization only if the European Commission has decided that the other country or international organization guarantees an adequate level of protection with a view to various issues (including respect for human rights and fundamental liberties and the effective functioning of the regulatory authorities).

In the absence of such a decision of adequacy,[2] RAM may only transfer personal data if it has provided adequate guarantees[3] and on the condition that the data subjects have enforceable rights and effective means of appeal.

RAM Active Investments S.A.: for clarity purposes Switzerland is considered by the European Commission a country providing adequate level of protection.

2.2. Rights of data subjects

2.2.1. Information on processing

In accordance with the principles of transparency, fairness, limited purposes and data retention, the data subjects, when their personal data is collected, receive clear information (the "**Information**") regarding: i) the identity of RAM and of the Data Protection Team (the "DPT"), ii) the characteristics of the processing and iii) the data subject's rights. The Information will be available through RAM's website and can be directly submitted to a data subject upon request.

2.2.2. Rights of access, rectification, erasure, portability and objection

The procedures must ensure compliance with the principles of accuracy and data retention, providing that each data subject is entitled to obtain:

(i) Right to access and request a copy of the data subject's personal data. Right to information on the processing activities of the relevant personal data.

(ii) Amendment of inaccurate personal data regarding them, or addition to such data if the data are incomplete;

(iii) Erasure, if certain conditions apply, e.g. if the data are no longer necessary for the purposes for which they were collected, if the data subject has withdrawn his/her consent or has exercised his/her right to object to the processing in case of direct marketing, or if the personal data have been processed unlawfully;

---

[2] Pursuant to Directive 95/46/EC, a total of fourteen countries were decided to be adequate: Andorra, Argentina, Australia, Canada, Faroe Islands, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland, Uruguay and the United States (from 2016 – Privacy Shield).

[3] E.g. the data protection clauses adopted by the European Commission ("standard contractual clauses").

(iv) Portability of the data being processed, in a structured, commonly-used format which is legible from an automatic instrument, if the processing is based on consent and is carried out by automated means;

(v) Withdrawal of consent for the specific data processing it was previously provided

RAM will ensure that following each request, the necessary information is provided to the data subjects in concise and accessible format, using simple and clear language, within one month (or two months in particularly complex cases), even in the event that the request is refused for due reasons.

2.3. Record of processing activities, risk analysis and data protection impact assessment (DPIA)

Register: RAM maintains a "record of processing activities" according to article 30 of the GDPR.

Risk analysis and DPIA: in order to ensure the integrity and confidentiality of the personal data, a risk analysis is performed for every processing activity entered in the record. Where this analysis shows that the processing may entail a high level of risk for the rights and freedoms of the data subject, a Data Protection Impact Assessment ("DPIA") is to be performed, subject to prior consultation with the DPT.

Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, RAM as controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

In deciding whether or not it is necessary to perform a DPIA in respect of a given processing, RAM will take into account the existence of the below aspects:

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

- processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences; or

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

2.4. Processing security

In order to guarantee a level of security for the processing which is commensurate with the risk, the procedures must define technical and organizational measures, taking into account the state of progress and implementation costs relative to the risks associated with the processing and the nature of the personal data, in accordance with the "privacy by design" and "privacy by default" principles. Such measures may include:

- Pseudonimization and encryption of personal data;

- Confidentiality and integrity of systems and processing services ensured on a permanent basis;

- Testing mechanisms and assessment of their effectiveness

- Restrictions of access, processing and/or extraction of personal data .

Taking account of the risks presented by the processing, which involve in particular the destruction, loss or unauthorized alteration of personal data, RAM will continuously supervise the security measures to guarantee an adequate level of protection for the personal data by default and before the personal data are processed.

2.5. Management of data breach events

In order to ensure that the principles of integrity and confidentiality of personal data are complied with, if a security breach is identified, whether accidental or unlawful, which entails the destruction, loss, alteration, or unauthorized disclosure of the data, thereby compromising their confidentiality, availability or integrity, the procedures must ensure, subject to prior involvement of the DPT, that the regulatory authority is notified within 72 hours of the time when the breach was noted. Such notification must contain the following information:

- The DPT's contact data;
- The nature of the personal data breach, with the information required by the Authority in charge[4]. Where possible it will include the categories and approximate number of parties involved;
- The likely consequences of the breach;
- The measures adopted or which are proposed to be taken in order to address the breach and mitigate its possible negative effects.

If the notification is not made within 72 hours, the reasons for the delay must be stated.

In cases where the breach may entail high risks for the rights and freedoms of the data subjects, the procedures must stipulate that – subject to prior consultation with the DPT – information be provided to the data subjects on the breach without unjustified delay. Such information is not necessary if it would require a disproportionate effort or if adequate technical and organizational data protection measures have been adopted (e.g. encryption).

The data breach procedure establish that: (i) the choice of the means of communication must take into consideration the access which the data subjects have to different formats, and where necessary, the linguistic diversities of the recipients; and that (ii) each breach of personal data, suspected or proven, must be adequately entered and documented in the register of breaches, to ensure that the accountability principle is complied with.

3 Scope of application and Group model

The GDPR scope of application within RAM Group is as follows:

- RAM Active Investments (Europe) S.A., as the party responsible for processing the personal data (e.g. of clients, staff etc.) in the European Union, apply the provisions of the GDPR in full, along with those of the related Luxembourg regulations;
- RAM Active Investments S.A. is established in Switzerland; however, it applies GDPR whenever it is required due to the scope of the relevant activity.

In some cases, RAM Active Investments (Europe) S.A. and RAM Active Investments S.A. may be categorised as joint controllers.

[4] The Luxembourg Authority has issued a standard form with all information to submit. In the event that the submission is to be done to another authority who has not issued a specific form, the report will be inspired from the Luxembourg form.

4 Organizational model

In accordance with the provisions of the regulations in force, the roles and responsibilities defined in connection with the organizational model adopted by RAM to manage personal data is set out below.

The **Board of Directors** assumes the general responsibility of direction and supervision for matters pertaining to personal data management via:

- Approval of this Policy and any other related policy, procedure or strategic decision;
- Appointment of the Data Protection Team (DPT).

The **Data Protection Team** performs amongst others the following activities:

- Advice to senior management and the other teams regarding the obligations deriving from the GDPR;
- Supervision of, and compliance with, the regulations on personal data protection;
- Review compliance of internal policies with GDPR principles;
- Determining the risk of the processing activities and the need of a Data Protection Impact Assessments. Performance of the DPIA when required;
- Co-operating with the regulatory authorities.

The DPT, is common to the RAM entities as it is easily accessible from each RAM entity and will operate independently avoiding any conflict of interest. This Team is composed of members from Compliance, IT, Investor Relations and Marketing Intelligence to ensure a transversal and entire coverage.

The relevant **HR & Organizational** functions together with the Data Protection Team will prepare and review the training programmes implemented to ensure that staff members are up-to-date at all times on privacy issues. The staff will be informed of their rights, processing activities and will be asked for consent whenever it is needed.

The **IT & Governance** functions together with DPT will i) perform the assessment of the impact on the rights and freedoms of the data subjects, ii) identify and adopt the most suitable and appropriate security measures to ensure compliance with the regulations in force.

All **staff members** are responsible for proper management of the personal data processed by them, and for compliance with the provisions of the Policy and the internal regulations.

Annex 1 – Principal definitions

Personal data	All information relating to natural persons who can be identified, directly or indirectly, from data which refer to them. For instance, this definition of personal data to be protected includes general and economic data, images and identification codes attributable to a natural person.
Special categories of data	Data which is able to reveal the racial or ethnic origin of a natural person, their political opinions, religious or philosophical beliefs or trade union affiliation.
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.

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.
Joint controller	The natural or legal person who, jointly with one or more controllers, determines the purposes and means of the processing. Joint controllers their respective areas of responsibility and duties in a written agreement.
Processor	A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. The processor is appointed by the controller if data has to be processed on the controller's behalf.
Sub-processor	A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller, once the controller has obtained authorization in writing, whether specific or general.
Data Protection Officer (DPO)	The natural person to be appointed as controller and processor, in specific cases (e.g. if the controller's or processor's principal activities consist of processing which, by its nature, scope of application and/or purpose, requires regular and systematic monitoring of the data subjects on a large scale).
Representative	A natural or legal person established in the European Union who, designated in writing by a controller/processor not established in the EU, represents them with regard to their respective obligations under the GDPR
Profiling	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 person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
Pseudonimization	The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures.
Encryption	Means of converting an original text into an apparently random sequence of letters, numbers and special symbols which only the person in possession of the correct decryption key would be able to reconvert to the original text.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.
Supervisory authority	An independent public authority which is established by a Member State to be responsible for monitoring the application of the General Data Protection Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data.
Staff	Every RAM staff member employed under a permanent or non-permanent, full-time or part-time contract, or under agency or staff leasing arrangements, interns and collaborators, including at the international branches.