GENERAL DATA PRIVACY POLICY

CONTENTS

1. POLICY OBJECTIVES AND SCOPE

Kamet is committed to maintaining the privacy of data obtained in the course of its business activities and complying with applicable laws and regulations (including the General Data Protection Regulation – GDPR – and the Loi Informatique et Libertés) regarding the processing of Personal Data.

This Genera Data Privacy Policy (hereinafter the "**Policy**") objectives are to ensure that Kamet adequately protects the Personal Data of clients and other persons obtained during their business activities, to minimise the risk of Kamet breaching applicable data privacy and protection laws and regulations (including the General Data Protection Regulation – GDPR – and the Loi Informatique et Libertés) and minimise the potential for penalties and damage to Kamet's reputation.

This Policy may be updated to reflect changes in applicable laws and regulations.

This Policy applies to Kamet group entities and incubated projects within Kamet.

2. DATA PROTECTION PRINCIPLES AND REQUIREMENTS

2.1 Lawfulness and transparency of processing

2.1.1 Lawfulness of processing

Kamet ensures that any processing of data it carries out is lawful.

The main legal basis under which Kamet relies on are when the processing is necessary for:

- performing a contract with a Data Subject or taking steps preparatory to a contract;
- complying with a legal obligation;
- achieving a legitimate interest of Kamet or a third party. While doing so, Kamet ensures that this interest does not override the interests, freedoms and human rights of the Data Subject. In such case, Kamet will balance interests before processing data on such legal basis.

Where such above conditions are not applicable, Kamet will seek to collect the consent of the individuals and will provide them with all the information required so as to obtain their consent.

Eventually, Kamet may also be allowed to process Personal Data when it appears necessary:

- to safeguard the vital interests of the person concerned or of another person;
- for the performance of a task carried out in the public interest.

Kamet will furthermore ensure that no processing of Personal Data is carried out if neither of those conditions apply.

2.1.2 Transparency of processing

Kamet ensures that Personal Data processing activities are carried out in a visible and transparent matter.

Where Kamet processes Personal Data, it will ensure that, where required, individuals are made aware that their Personal Data are being collected, the purpose of the processing is specified, and it will be specified whether data will be shared with any allowed third parties or transferred to third countries.

Kamet will also make Data Subjects know for how long their Personal Data are likely to be retained in order to achieve the purpose, or at least on which criteria this retention period relies on.

Kamet will always provide Data Subjects with the details of the person to contact and the procedures to follow to exercise their rights under the GDPR.

This information can be transmitted to the Data Subject by legal notice forms, notice board, websites legal notices, contracts, personalized letter or email, employees application form. Transparency also involves notification to Data Subject of any change of purpose of the processing.

For any processing activity, the necessity of including a privacy notice will always be considered by Kamet.

2.1.3 Accountability

Kamet commits to ensure compliance with the principles detailed in this Policy and will take steps to demonstrate that these principles are respected by means of tangible evidences.

These compliance measures include the implementation of appropriate policies, actions of training and awareness-raising of employees, the implementation of an appropriate governance model, including the designation of a Data Protection Officer (or a person responsible for data privacy matters) within Kamet and its incubated projects.

2.2 Purpose limitation of processing

Kamet ensures that the Personal Data will be processed only pursuant to three principles with respect to their purpose:

- Specified purpose: that is to say that the purpose shall be determined,
- Explicit purpose: that is to say that the purpose shall be explained in clear and comprehensible terms
- And a legitimate purpose: that is to say that the purpose shall have a legal basis (see above, section 2.1.1 “Lawfulness of Processing”).

Kamet only processes Personal Data to achieve a given purpose and will not process such data further in a way incompatible with the initial purpose. In such cases, Kamet will enforce appropriate steps to provide the suitable information or, when required, obtain the prior consent of the Data Subjects.

Being specific and explicit about the purposes will also allow Kamet to determine the right kind and type of information that Kamet may have to provide further to Data Subjects (see above, section 2.1.2 “Transparency”)

2.3 Relevance and accuracy of data

2.3.1 Data relevance

Kamet processes Personal Data which are adequate, relevant and not excessive in relation to the purpose(s) for which they are collected and/or further processed:

- “Adequate” means that the Personal Data processed are useful to fulfill the purpose of the processing

- "Relevant" means that the Personal Data processed are the one which are necessary to fulfill the purpose of the processing
- "Not excessive" means that the Personal Data processed are necessary for the purpose of the processing

In particular, Kamet ensures the Personal Data collection forms do not ask for more Personal Data than what is actually needed.

2.3.2 Data accuracy

In addition, Kamet ensures that the Personal Data processed are accurate and complete for the purpose(s) concerned:

- "Accurate" means that Personal Data are up-to-date
- "Complete" means that all Personal Data needed are processed

Enforcing such principles is crucial for Kamet while conducting business with its clients and suppliers, as well as towards its employees.

2.4 Storage limitation of data

Kamet does not retain Personal Data for longer than it is necessary to achieve the purposes for which they were obtained unless otherwise required by applicable laws.

In practice, Kamet shall determine the maximum data retention period with the following criteria:

- Business needs;
- Legal obligations;
- Data Protection Authority's recommendations;
- Best practices.

To learn more, please refer to Kamet's Personal Data Retention Policy.

2.5 Enforcement of Data Subject rights

Kamet shall implement procedures to ensure prompt responses to Data Subject requests to exercise their rights, and more specifically:

- **The right of access:** to request Kamet for information about his/her own Personal Data including information relating to how Personal Data had been collected, the list of recipients or categories of recipients to which their Personal Data is transferred (if applicable), the purpose(s) of the collection of their Personal Data and of their transfer (if applicable), or any other information which would be required under applicable local law

- **The right to rectification:** to ask Kamet to rectify data, when it's inaccurate

- **The right to erasure:** to request for the deletion of his/her own Personal Data (if legally possible and on legitimate grounds)

- **The right to restriction of processing:** to request blocking of any further processing

- **The right to data portability**: to obtain and reuse his/her own Personal Data for his/her own purpose across different services in a way that is portable and safe

- **The right to object:** to object to a Data Processing on legitimate grounds

In order to exercise their rights as described above, Data Subjects should be provided with the contact information of the person in charge (Data Protection Officer or the person responsible for data privacy matters).

Any request should be handled within a reasonable period of time and without undue delay and in any event within one month of receipt of the request (this period may be extended by two additional months where necessary, taking into account the complexity and number of the requests).

Where still dissatisfied after the response made, individuals must be made aware of their right to complain to a supervisory authority and to seek a judicial remedy.

To learn more, please refer to Kamet's Data Subject Rights Procedure.

2.6 Privacy by design

2.6.1 Privacy by design

According to the Privacy by Design principle, Kamet endeavours to prevent risks on Data Processing from occurring, at the earliest stage possible, before the data processing begins.

This means Kamet ensures that the suitable organizational and technical measures are taken so as to have in place the appropriate level of protection for each processing activity.

Kamet will enforce Privacy by design as a business model and accompany the processing from beginning to end, just as it will accompany Personal Data through its lifecycle.

During the processing, internal audits (or external audits when auditing processors) are carried out. At the end of processing, Personal Data are securely destroyed or anonymised.

Kamet Personal Data policies and procedures take into account Privacy by Design culture and promote it to the staff, partners and incubated projects of Kamet.

All the new projects will take the Privacy by Design principles into account and the principles will be integrated into the various existing project methodologies.

To learn more, please refer to the Kamet's Privacy by Design Guide.

2.6.2 Data Protection Impact Assessment

Kamet conducts risk analyses or, when required, Data Protection Impact Assessments, to analyse the potential risks at stake with any new project.

When applicable, the Data Protection Impact Assessment is carried out prior to the processing; meaning before the project is operationally deployed and Kamet starts collecting and/or processing data.

Operationally, each department owner of a project is responsible to ensure the Data Protection Impact Assessment is carried out.

The resulting analysis will let Kamet know which safety measures need to be implemented before launching the project, and the degree of security Kamet needs to achieve depending on the level of the risk presented by the project.

Where the Data Protection Impact Assessment results indicate that the processing would result in a high risk in the absence of measures taken by Kamet to mitigate the risk, Kamet may consult the supervisory authority prior to processing.

2.7 Organisational and security measures

2.7.1 Security

Whether Kamet or the incubated projects are considered as Data Controller or Data Processor for a processing, it is required by the GDPR to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk.

These security measures must ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services in order to avoid unlawful destruction, loss, alteration and unauthorized disclosure.

These measures can be physical, technical or it can consist in a security plan but must ensure a level of security appropriate to the risks represented by the Data Processing and the nature of the Personal Data to be protected.

All employees or contractors must follow Kamet security procedures as well as the Data Breach notification when it occurs to be necessary.

When processing is carried out by a Processor, Kamet must select a Processor providing sufficient technical security and organizational measures to ensure that the processing will be carried out in accordance with legal requirements.

To learn more, please refer to Kamet's IT Security Policy.

2.7.2 Data Transfer

Kamet, its entities and its incubated projects, located or not in Europe, can outsource many activities. This outsourcing of services can imply cross borders transfers, data transfers overseas, including data exchanges between Kamet and its incubated projects or entities.

The three usual transfer cases that may be met are transfers:

- To/From a company located in the European Union (or a country considered to have an adequate level of data privacy by the European Commission)
- To/From Kamet to one of its incubated projects
- To/From a third party (e.g. a service provider, a subcontractor…) located in another part of the world.

Under the GDPR, the rules differ between data transfers within the European Union (or a country considered to have an adequate level of data privacy by the European Commission) and data transfers

out of the European Union in a country considered to have an inadequate level of data privacy by the European Commission.

Kamet shall ensure that all transfers of Personal Data outside the European Union in a country considered to have an inadequate level of data privacy by the European Commission are covered by appropriate safeguards that ensure an adequate level of protection for the rights and freedoms of Data Subjects such as:

- Standard data protection clauses adopted by the European Commission
- Standard data protection clauses adopted by a supervisory authority and approved by the European Commission
- An approved code of conduct

2.7.3 Data Protection Authority

Kamet shall cooperate with the relevant Data Protection Authority any time it will be required to do so.

The relevant Data Protection Authority is the one concerned by the processing of Personal Data because:

- Kamet or one of its incubated project is established on the territory of the Member State of that Data Protection Authority;
- Data Subjects residing in the Member State of that Data Protection Authority are substantially affected or likely to be substantially affected by the processing; or
- a complaint has been lodged with that Data Protection Authority.

Inquiries by Data Protection Authorities must always be reported to the Data Protection Officer (or the person responsible for data privacy matters) at :

Kamet - Data Protection Officer

58 rue de Prony 75017 Paris

dpo@kametventures.com

2.8 Reporting of Personal Data Breaches

A Personal Data Breach is 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.

Usually, a Personal Data Breach happens when Personal Data is disseminated without authorization, e.g. stolen, lost or mistakenly disclosed.

Any individual who discovers a Personal Data Breach must inform the DPO at dpo@kametventures.com.

As a Personal Data Breach might be a risk for rights and freedoms of individuals, please be aware that Kamet may be required to notify a Personal Data Breach to the relevant Data Protection Authority within 72 hours after having become aware of it and/or to the Data Subjects without undue delay.

To learn more, please refer to Kamet's Personal Data Breach Procedure.

3. ROLES AND RESPONSIBILITIES

The CEO of Kamet is ultimately responsible for ensuring that the company establishes policies and procedures consistent with this Policy within his/her business and meeting applicable legal, regulatory or contractual requirements.

The management of the data privacy within Kamet follows a “two lines of defense” model:

- The Management (the first line of defense) is responsible for ensuring Personal Data handling procedures are meeting local requirements and are consistent with this Policy;
- The DPO (the second line of defense) supports the Management by means of developing and implementing adequate procedures, safeguards and controls to ensure meeting local requirements and consistency with this Policy.

3.1 Roles and responsibilities of the Management

The Management (i.e. Management who decides what, why and how Personal Data is collected and processed) as well as the Data Controller are responsible for understanding the applicable regulatory requirements and ensuring that Kamet's collection, processing, transfer and retention of Personal Data comply with those regulatory requirements and this Policy.

The Management should provide the DPO (or, to a certain extent, the person responsible for data privacy matters) with the necessary information and means to enable him to support them in ensuring Kamet’s compliance with this Policy and local requirements. In particular, the Management should have regular exchanges with the DPO (or, to a certain extent, the person responsible for data privacy matters) and keep him/her informed about relevant organisational or other developments that may have an impact on Data Privacy.

Also, the Management should ensure appropriate “tone at the top” communication with respect to awareness of the issues covered by this Policy.

3.2 Roles and responsibilities of the DPO

Kamet must appoint a DPO with appropriate authority, resources and skills to support the Management in ensuring Kamet’s compliance with this Policy and relevant local requirements. The DPO is the initial contact person for any Data Privacy matters or issues.

3.3 Roles and responsibilities of the person responsible for data privacy matters

Where it is not mandatory to appoint a Data Protection Officer, it is still recommended to appoint a person responsible for data privacy matters. While this person doesn’t benefit from the same status as the Data Protection Officer, he/she must be involved in all matters where the DPO is meant to be involved.

4. HOW TO DETERMINE WHO IS DATA CONTROLLER OR DATA PROCESSOR

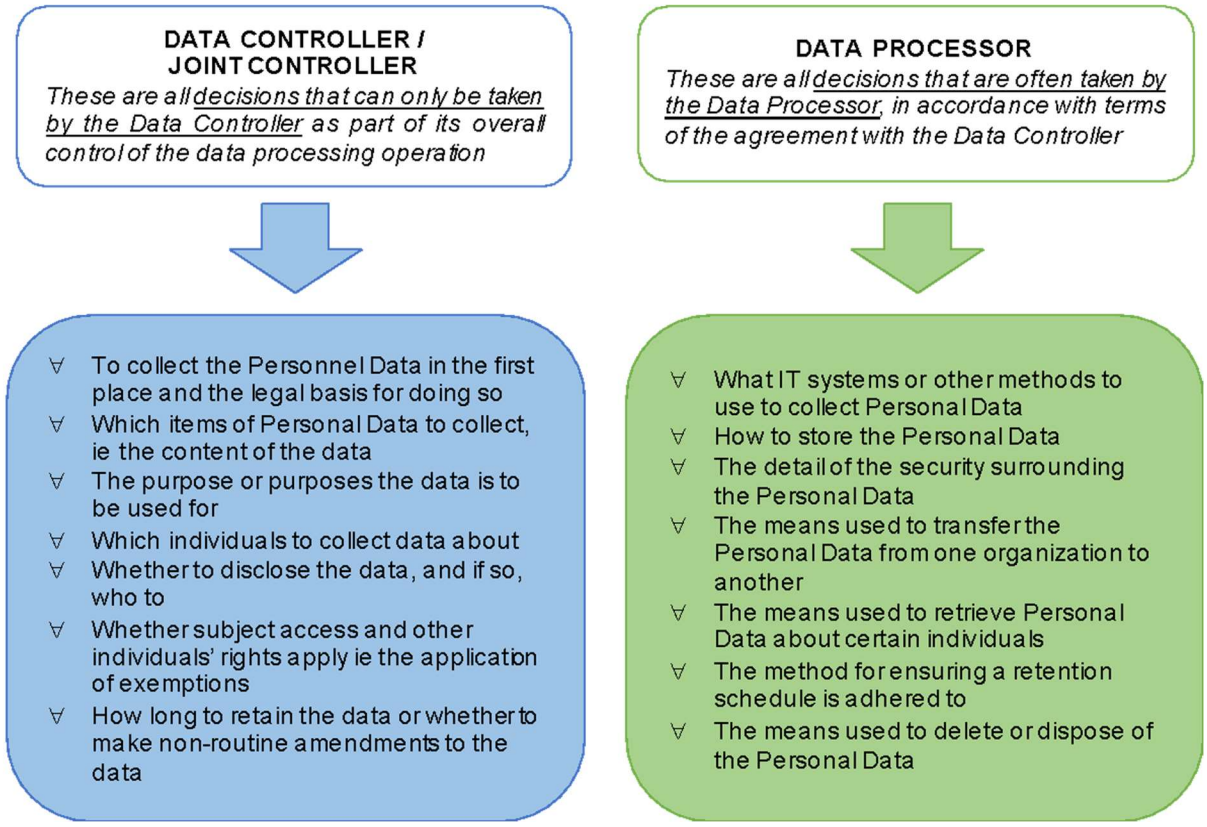
For each Data Processing, there is at least one Data Controller who determines the purpose, conditions and means of the Data Processing. If another legal entity is involved in the Data Processing (e.g. by jointly determining the purpose of the Data Processing with the Data Controller, by processing the Personal Data under the Data Controller's instructions…), it can be qualified either as Joint Data Controller or as Data Processor.

When Kamet is involved in the processing of Personal Data, it is essential to be able to determine whether it is acting as a Data Controller or as a Data Processor as they bear different contractual and regulatory obligations.

The fact that Kamet provides a service to another legal entity does not necessarily mean that it is acting as a Data Processor. It could also be a Data Controller, depending on the degree of control it exercises over the processing operation. In any cases, a legal entity cannot be both Data Controller and Processor for the same data processing activity.

Where Kamet is Joint Controller, the roles and responsibilities of Kamet and the other Data Controller should be clearly defined and set up in contract.

The differences between Data Controller, Joint Controller and Data Processor are illustrated in the non-exhaustive list below:



APPENDIX I – DEFINITIONS

Data Controller: any person or legal entity, that alone, severally or jointly, determines the purposes, conditions and means of a Data Processing.

Data Processing: any action taken in conjunction with data such as collection, recording, copying, reproduction, transferring, searching, sorting, separating, crossing, merging, modification, provisioning, usage, disclosure, dissemination, saving, organizing, storing, adjusting, disclosure by transmission or otherwise making available, hiding, moving and otherwise making unavailable, as well as implementation of other actions in connection with the data, regardless of whether it is performed automatically, semi-automatically or on paper format.

Data Processor: any person (but not an employee of the Data Controller) or legal entity, that processes Personal Data on behalf and under the instructions of the Data Controller.

Data Protection Officer ("DPO"): a person responsible for ensuring the entity's compliance with applicable legal and regulatory data privacy requirements.

Data Recipient: a natural or legal person, public authority, agency or another body, to which the Personal Data are disclosed, whether a third party or not. However, public authorities which may receive Personal Data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.

Data Subject: an individual who is the subject of the 'Personal Data' and can be identified or distinguished from others, directly or indirectly, by means reasonably likely to be used by any natural or legal person, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

Data Subject Request: means a request made by an individual and related to Personal Data only.

Data Transfer: data communication, reporting, copy, through a telecommunications network or similar technical system from one format to any another one to a third party for processing purposes. (e.g. intra group HR databases pooling systems, transfer to a service provider for computerized data entry, use of foreign call center, data hosting, computer platforms operating, international IT maintenance).

General Data Protection Regulation (GDPR): means the EU regulation 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.

Personal Data: any information relating to an individual who is or can be identified either from the data or from the data in conjunction with other information, by reference to an identification number or to one or more factors specific to him, *e.g. a person's full name, email or postal address, phone number, physical characteristics, health or personnel records, financial/bank account information, contract number, etc*. Personal Data is each piece of information related to the individual, regardless of the form in which it is expressed and the format of the information holder, *e.g. storage media, paper, tape, film, electronic media, etc.*

Personal Data Breaches: a security breach affecting Personal Data. This term is used to designate situations in which the security of Personal Data has been or could be compromised. This could include the disclosure, copy, transmission, access, removal, destruction, theft or use of Personal Data by unauthorised individuals, whether accidentally or intentionally.

Retention Period: the amount of time a record is required to be kept following the collection after which it will need to be disposed (maximum retention time).

Special Categories of Data: means racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.