Data Protection Policy

General Data Protection Regulation (EU) 2016/679 (GDPR)

Contents

1. Introduction

The General Data Protection Regulation (GDPR) is a comprehensive regulation, which unifies data protection laws across all European Union member states. It defines an extended set of rights for European Union citizens and residents regarding their personal information. Consequently, it describes strict requirements for companies and organizations on collecting, storing, processing and managing personal data.

Red Mars Capital Ltd. (hereinafter referred to as the "Company") is committed to protecting the rights and safely and securely processing the Clients` data, in accordance with all legal obligations. The Company holds personal data about its employees, clients, suppliers and other individuals for a variety of Business purposes.

2. Definitions

"Business purposes" - the purposes for which personal data may be used by us: personnel, administrative, financial, regulatory, payroll and business development purposes.
Business purposes include the following:

- Compliance with our legal, regulatory and corporate governance obligations and good practice
- Gathering information, as part of investigations by regulatory bodies or in connection with legal proceedings or requests
- Ensuring business policies are adhered to (such as policies covering email and internet use)
- Operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of commercially sensitive information, security vetting, credit scoring and checking
- Investigating complaints
- Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments
- Monitoring staff conduct, disciplinary matters
- Marketing our business
- Improving services

"**Consent"** of the data subject, means any freely given, specific, informed and explicit indication, of the Client`s wishes, by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data, relating to him or her;

"Data controller" - means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by law

"**Data processor" -** means a natural or legal person, public authority, agency or other body, which processes personal data on behalf of the controller.

"Personal data" - means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one, who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an

online identifier or to one or more factors, specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

The Personal data we gather, may include: individuals' phone number, email address, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, and CV.

"**Processing" -** means 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.

"Special categories of personal data" - include information about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences, or related proceedings, and genetic and biometric information —any use of special categories of personal data should be strictly controlled in accordance with this policy.

"**Supervisory authority" -** This is the national body responsible for data protection. The supervisory authority for the Company is **Commissioner for Personal Data Protection,** located at 1 Iasonos Street, 1082 Nicosia
P.O. Box 23378, CY-1682 Nicosia
Tel. +357 22 818 456, Fax +357 22 304 565
e-mail: commissioner@dataprotection.gov.cy
Website: http://www.dataprotection.gov.cy/
Member: **Ms Irene Loizidou Nikolaidou**

Contact details of the Data Protection Officer (DPO) of the Commissioner's Office
Email dpo@dataprotection.gov.cy

3. Scope of the policy

This policy applies to all staff, who must be familiar with this policy and comply with its terms.

This policy outlines the procedures, which the Company seeks to protect personal data and ensures, that the staff understand the rules, governing the use of the personal data, which they have access to, during the course of their work. In particular, this policy requires staff to ensure, that the appointed Data Protection Officer (DPO), if any, will be consulted before any significant new data processing activity is initiated, to ensure that relevant compliance steps are addressed.

This policy supplements other Company`s policies, relating to internet and email use.

The Company reserves its right to supplement or amend this policy by additional policies and guidelines from time to time, if necessary. Any new or modified policy will be circulated to the staff before.

4. The 6 principles relating to processing of personal data

The Company shall make every effort possible, to strictly comply with the principles of data protection (the "Principles"), enumerated in Chapter II, Article 5 of the EU General Data Protection Regulation. The Principles are:

1. Lawful, fair and transparent - data collection must be fair, for a legal purpose and the Company must be open and transparent, as to how the data will be used
2. Limited for its purpose - data can only be collected for a specific purpose
3. Data minimisation - any data collected, must be necessary and not excessive for its purpose.
4. Accurate - the data the Company holds, must be accurate and kept up to date
5. Retention – the Company cannot store data, longer than it`s necessary.
6. Integrity and confidentiality - the data the Company holds, must be kept safe and secure

5. Accountability and transparency

Accountability and transparency must be ensured in all use of personal data. The Company and the relevant staff, who have access to personal Clients` or employees` data, shall keep a record of all the data processing activities they are responsible for, and confirming its compliance with each of the Principles. This information must be kept up to date.

To comply with data protection laws and the accountability and transparency Principles of GDPR, the Company must demonstrate compliance. Each department must understand its particular responsibilities, and to ensure how these would meet the following data protection obligations:

- Fully implement all appropriate technical and organisational measures;
- Maintain up to date and relevant documentation on all processing activities;
- Conducting Data Protection Impact Assessments;
- Implement measures to ensure privacy by design and default, including:
    - Data minimisation
    - Transparency
    - Allowing individuals to monitor processing
    - Creating and improving security and enhanced privacy procedures on an ongoing basis

6. Our procedures

6.1 Fair and lawful processing

The Company must process personal data fairly and lawfully, in accordance with individuals' rights under the first Principle. This generally means, that the Company should not process personal data, unless the individual, whose details are processing, has consented to this happening, as per the requirements in Article 6(1)(a) & Article 7(1) of the GDPR.

If the Company cannot apply a lawful basis, this means, that the processing does not conform to the first principle and will be unlawful. The Clients have the right to have any data unlawfully processed erased.

6.2 Controlling vs. processing data

The Company is classified as a data controller and it is lawfully controlling data, adhering to all applicable regulations and Laws.

6.3 Lawful basis for processing data

The Company must ensure, that any data it is responsible for managing, has a written lawful basis and that all actions comply with the lawful basis. At least one of the following conditions must apply, whenever personal data is being processed:

6.3.1. Consent

The Company should hold recent, clear, explicit, and defined consent for the individual's data to be processed for a specific purpose.

6.3.2. Contract/ Client`s Agreement

The processing is necessary to fulfil or prepare a contract for the individual.

6.3.3. Legal obligation

The Company have a legal obligation to process the data (excluding a contract).

6.3.4. Vital interests

Processing the data is necessary to protect a person's life or in a medical situation.

6.3.5. Public function

Processing necessary to carry out a public function, a task of public interest or the function has a clear basis in law.

6.3.6. Legitimate interest

The processing is necessary for our legitimate interests. This condition does not apply, if there is a good reason to protect the individual's personal data, which overrides the legitimate interest.

6.4 Defining lawful basis

If you are assessing the lawful basis, you must first establish, that the processing is necessary. This means the processing must be a targeted, appropriate way of achieving the stated purpose. You cannot rely on a lawful basis, if you can reasonably achieve the same purpose by some other means.

Please note, that more than one basis may apply, and you should rely on what will best fit the purpose, not what is easiest.

<u>Consider the following factors and thereafter the answers:</u>
What is the purpose for processing the data?
Can it reasonably be done in a different way?
Is there a choice as to whether or not to process the data?
Who does the processing benefit?
After selecting the lawful basis, is this the same as the lawful basis the data subject would expect?
What is the impact of the processing on the individual?
Are you in a position of power over them?
Are they a vulnerable person?
Would they be likely to object to the processing?

Are you able to stop the processing at any time on request, and have you factored in how to do this?

Moreover, the Company should ensure, that the Clients whose data is being processed, are informed of the intended purpose for the collection of data. This should occur via a privacy notice. This applies, whether the Company have collected the data directly from the Client, or from another source.

7. Special categories of personal data

Previously known as sensitive personal data, this means data about an individual, which is more sensitive, so requires more protection. This type of data could create more significant risks to a person's fundamental rights and freedoms, for example by putting them at risk of unlawful discrimination. The special categories include information about an individual's: race, ethnic origin, politics, religion, trade union membership, genetics, biometrics (where used for ID purposes), health, sexual orientation

In most cases, where and if the Company process special categories of personal data, it will require the Client`s *explicit* consent to do this, unless exceptional circumstances apply or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work). Any such consent will need to clearly identify, what the relevant data is, why it is being processed and to whom it will be disclosed.

The condition for processing special categories of personal data must comply with the law. If we do not have a lawful basis for processing special categories of data, that processing activity must cease.

8. Responsibilities

8.1 Company`s responsibilities:

- Analysing and documenting the type of personal data it holds;
- Checking procedures to ensure, they cover all the rights of the individual;
- Identify the lawful basis for processing data;
- Ensuring consent procedures are lawful;
- Implementing and reviewing procedures to detect, report and investigate personal data breaches;
- Store data in safe and secure ways;
- Assess the risk, which could be posed to individual rights and informs should data be compromised;

8.2 Staff responsibilities:

- Fully understand your data protection obligations;
- Check that any data processing activities you are dealing with, comply with our policy and are justified;
- Do not use data in any unlawful way;
- Do not store data incorrectly, be careful with it or otherwise cause us to breach data protection laws, and our policies through your actions;
- Comply with this policy at all times;

- Raise any concerns, notify any breaches or errors, and report anything suspicious, or contradictory to this policy, or our legal obligations without delay;

8.3 Responsibilities of the Data Protection Officer (DPO), if any is appointed:

- Keeping the board updated about data protection responsibilities, risks and issues;
- Reviewing all data protection procedures and policies on a regular basis;
- Arranging data protection training and advice for all staff members and those included in this policy;
- Answering questions on data protection from staff, board members and other stakeholders;
- Responding to individuals such as clients and employees, who wish to know, which data is being held by the Company;
- Checking and approving with third parties, which handle the Company's data any contracts or agreement, regarding data processing;

8.4 Responsibilities of the IT Manager:

- Ensure all systems, services, software and equipment meet acceptable security standards;
- Checking and scanning security hardware and software regularly, to ensure it is functioning properly;
- Researching third-party services, which the company is considering using to store or process data;

8.5 Responsibilities of the Compliance Officer

- Approving data protection statements attached to emails and other marketing copy;
- Addressing data protection queries from clients, target audiences or media outlets;
- Coordinating with the DPO to ensure all marketing initiatives adhere to data protection laws and the company's Data Protection Policy;

9. Accuracy and relevance

The Company shall ensure, that any personal data, which is being processed, is accurate, adequate, relevant and not excessive, given the purpose, for which it was obtained. The Company shall not process personal data obtained for one purpose for any unconnected purpose, unless the Client concerned, has agreed to this or would otherwise reasonably expect this.

Clients may request modification in inaccurate personal data, relating to them. If information is considered as being inaccurate, then this fact should be brought to the attention of the DPO.

10. Data security

All personal data should be kept secure against loss or misuse. Where other organisations process personal data, as a service on our behalf, the DPO, if any is appointed, will establish what, additional specific data security arrangements need to be implemented in contracts with those third-party organisations.

10.1 Storing data securely

In cases, when data is stored on printed paper, it should be kept in a secure place, where unauthorised personnel cannot access it. Printed data should be shredded, when it is no longer needed. Data stored on a computer, should be protected by strong passwords, which are changed regularly. All staff use a password manager to create and store their passwords.

Data stored on CDs or memory sticks, must be encrypted or password protected and locked away securely, when they are not being used. The DPO must approve any cloud used to store data. The server containing personal data is kept in a secure location and it is protected by security software. Data is regularly backed up in line with the Company's backup procedures, and it should never be saved directly to mobile devices such as laptops, tablets or smartphones.
All possible technical measures must be put in place to keep data secure.

10.2 Data retention

The Company retain personal data for no longer than it`s necessary. The period of retention depends on the circumstances of each case, taking into account the reasons, which the personal data was obtained for, but should be determined in a manner consistent with the data retention guidelines. Under Applicable Regulations, the Company shall keep records containing Clients` personal data, trading information, account opening documents, communications and anything else, which relates to the Client for at least five (5) years, after the termination of the Business Relationship with the Client.

Emanating from the new regulatory requirements, entered into force as of 2nd January 2018, upon expiry of the retention period referred above, the Company shall ensure, that it deletes personal data, unless otherwise provided for by national law, which shall determine, under which circumstances the Company may or shall further retain data.

After the Company have carried out a thorough assessment of the necessity and proportionality of such further retention and consider it to be justified, as necessary for the prevention, detection or investigation of money laundering or terrorist financing, the Company may be allowed to further retain data. That further retention period shall not exceed five (5) additional years.

10.3 Transferring data internationally

There are restrictions on international transfers of personal data. The Company shall not transfer any personal data abroad, or anywhere else outside of normal rules and procedures, without express permission from the DPO, or the respective officer responsible for the storing and safeguarding of the Clients` data.

11. Rights of individuals

All Clients have rights to their personal data, which the Company must respect and comply with to the best of its ability. We must ensure individuals can exercise their rights in the following ways:

11.1 Right to be informed

Providing privacy notices, which are concise, transparent, intelligible and easily accessible, free of charge, that are written in clear and plain language. Keep a record of how the staff use personal data to demonstrate compliance with the need for accountability and transparency.

11.2 Right of access
All Clients are able to access their personal data and supplementary information, to be aware of and verify the lawfulness of the processing activities.

11.3 Right to rectification
The staff should rectify or amend the personal data of the Client, if requested, because it is inaccurate or incomplete. This must be done without undue delay and in any event within one month of receipt of the request.

11.4 Right to erasure
The Company must delete or remove Clients` data if requested and there is no compelling reason for its continued processing.

11.5 Right to restrict processing
The Company must comply with any request to restrict, block, or otherwise suppress the processing of personal data. The Company is permitted to store personal data, if it has been restricted, but not process it further, and must retain enough data, to ensure the right to restriction is respected in the future.

11.6 Right to data portability
The Company must provide the Client`s data in a commonly used, machine-readable format, and send it directly to another controller or data processor, if requested.

11.7 Right to object
The Company shall respect the right of any Client to object data processing, based on legitimate interest or the performance of a public interest task, direct marketing, including profiling, or processing Client`s data for scientific and historical research and statistics.

11.8 Rights in relation to automated decision making and profiling
The Company shall respect the Clients` rights in relation to automated decision making and profiling, and their right to object to such automated processing, have the rationale explained to them, and request human intervention.

12. Privacy notices

12.1 When to supply a privacy notice
A privacy notice must be supplied at the time the data is obtained, if obtained directly from the Client. If the data is not obtained directly from the Client, the privacy notice must be provided within a reasonable period of having obtained the data, which mean within one month.
If the data is being used to communicate with the Client, then the privacy notice must be supplied at the latest, when the first communication takes place.
If disclosure to another recipient is envisaged, then the privacy notice must be supplied prior to the data being disclosed.

12.2 What to include in a privacy notice

Privacy notices must be concise, transparent, comprehensible and easily accessible. They are provided free of charge and must be written in clear and plain language.

The following information must be included in a privacy notice to all Clients:

- Identification and contact information of the data controller and the data protection officer;
- The purpose of processing the data and the lawful basis for doing so;
- The legitimate interests of the controller or third party, if applicable;
- The right to withdraw consent at any time;
- Any recipient or categories of recipients of the personal data;
- Detailed information of any transfers to third countries, if any, and safeguards in place;
- The retention period of the data or the criteria used to determine the retention period, including details for the data disposal after the retention period;
- The right to lodge a complaint and internal complaint procedures;
- Any existence of automated decision making, including profiling and information about how those decisions are made, their significances and consequences to the Client;
- Whether the provision of personal data is part of a statutory of contractual requirement or obligation, and possible consequences for any failure to provide the data (only for data obtained directly from the Client);

13. Subject Access Requests

13.1 What is a subject access request?

A Client has the right to receive confirmation, that their data is being processed, access to their personal data and supplementary information, which means the information, which should be provided in a privacy notice.

13.2 How we deal with subject access requests

The Company shall provide the Client with a copy of the information on request, free of charge. This must occur without delay, and within one month of receipt of the request. The Company shall endeavour to provide the Client with access to their information in commonly used electronic formats.
If complying with the request is complex or numerous, the deadline can be extended by two months, but the Client must be informed within one month. The Company shall obtain an approval from the DPO before extending the deadline.

The Company may refuse to respond to certain requests, and can, in circumstances of the request being manifestly unfounded or excessive, charge a fee. If the request is for a large quantity of data, the Company may request from the Client to specify the information they are requesting. This can only be done with express permission from the DPO.

Once a request has been made, the Company shall not change or amend any of the data, which has been requested. Doing so is a criminal offence.

13.3 Data portability requests

The Company shall provide the data requested in a structured, commonly used and machine-readable format. This would normally be a CSV file, although other formats are acceptable too. This data will

be provided either to the Client, who has requested it, or to the data controller. This must be done free of charge and without delay, and no later than one month. This can be extended to two months for complex or numerous requests, but the Client have to be informed of the extension within one month and accompanied with an express permission from the DPO.

14. Right to erasure

Clients have a right to have their data erased and for the processing of data to cease in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which, it was originally collected and/or processed;
- Where consent is withdrawn;
- Where the Client objects processing and there is no overriding legitimate interest for continuing the processing;
- The personal data was unlawfully processed or otherwise breached data protection laws
- To comply with a legal obligation;

The Company may only refuse to comply with the right to erasure in the following circumstances:

- To exercise the right of freedom of expression and information;
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority;
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes;
- The exercise or defence of legal claims

If personal data, which needs to be erased has been passed onto other parties or recipients, they must be contacted and informed of their obligation to erase the data. If the Client asks, the Company must inform them of those recipients.

15. The right to object

The Clients have the right to object to their data being used on grounds, relating to their particular situation. The Company shall immediately cease processing unless:

- We have legitimate grounds for processing, which override the interests, rights and freedoms of the Client;
- The processing relates to the establishment, exercise or defence of legal claims.

The Company shall in all instances inform the Clients of their right to object at the first point of communication, i.e. in the privacy notice.

The Company may only carry out automated profiling or decision making, which has a legal or similarly significant effect on the Client, only if it is necessary for the entry into or performance of a contract, it is based on the Client's explicit consent, or otherwise authorised by law.

In these circumstances, the company shall give to the Clients detailed information about the

automated processing, offer simple ways for them to request human intervention or challenge any decision about them.

16. Third parties

16.1 Using third party controllers and processors

As a data controller the Company must have written contracts in place with any third-party data controllers and/or data processors, which it is planning to enter into an agreement with. The agreement must contain specific clauses, which set out the Company`s and third-party liabilities, obligations and responsibilities.

As a data controller, the Company must only appoint processors, who can provide sufficient guarantees under GDPR and that the rights of data subjects will be respected and protected.

16.2 Contracts

The contracts must comply with the standards set out by the GDPR and, where possible, follow the standard contractual clauses, which are available. The contracts with third parties must set out the duration of the processing, the nature and stated purpose of the processing activities, the types of personal data and categories, and the obligations and rights of the third-party.

At a minimum, the contracts must include terms, which specify:

- Acting only on written instructions;
- Those involved in processing the data, are subject to a duty of confidence;
- Appropriate measures will be taken, to ensure the security of the processing;
- Sub-processors will only be engaged with the prior consent of the controller and under a written contract;
- The controller will assist the processor in dealing with data access requests and allowing the Clients to exercise their rights under GDPR;
- The processor will assist the controller in meeting its GDPR obligations, in relation to the security of processing, notification of data breaches and implementation of Data Protection Impact Assessments;
- Delete or return all personal data at the end of the contract;
- Submit to regular audits and inspections and provide whatever information necessary for the controller and processor to meet their legal obligations;
- Nothing will be done by either the controller or processor to infringe on GDPR;

17. Criminal offence data

Any criminal record checks are justified by law. Criminal record checks cannot be undertaken based solely on the consent of the subject. We cannot keep a comprehensive register of criminal offence data. All data relating to criminal offences is considered to be a special category of personal data and must be treated as such. You must have approval from the DPO prior to carrying out a criminal record check.

18. Audits, monitoring and training

18.1 Data audits
Regular data audits to manage and mitigate risks. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales, which may be relevant. The Company shall conduct a regular data audit, as defined by the DPO and normal procedures.

18.2 Monitoring
All employees must observe this policy. The DPO has overall responsibility for this policy. The Company shall keep this policy under review and amend or change it, as and if required. Any breaches of this policy must be notified to the DPO. The staff must comply with this policy fully and at all times.

18.3 Training
Adequate training on provisions of data protection regulation will be provided to all employees, customised according to their position. If an employee changes his/her position and/or responsibilities, and thereafter he/she is responsible for requesting new data, then a new data protection training, relevant to that new role or/and responsibilities will be provided.

19. Reporting breaches
Any breach of this policy or of data protection laws, must be reported as soon as practically possible. The Company has the legal obligation to report any data breaches to Commissioner for Personal Data Protection.

19.1 An obligation to report
All members of staff have an obligation to report actual or potential data protection compliance failures. This allows the Company to:

- Investigate the failure and take remedial steps, if necessary;
- Maintain a register of compliance failures;
- Notify the Commissioner for Personal Data Protection of any compliance failures, which are material either in their own right or as part of a pattern of failures;

19.2 Failure to comply
Any member of staff, who fails to notify of a breach, or is found to have known or suspected a breach has occurred, but has not followed the correct reporting procedures, will be liable to disciplinary action.

The Company takes compliance with this policy very seriously. Failure to comply puts both you and the organisation at risk.
The importance of this policy means, that failure to comply with any requirement may lead to disciplinary action under our procedures, which may result in dismissal.