DATA PROTECTION POLICY

Company Name: Mariner Finance plc

Company Number: C 31514

[Hereinafter referred to as the 'Company' and/or 'We' and/or 'Our']

Date: 22nd May 2018

Contents

1. Introduction

In view of the business and the industry in which we operate, the Company holds personal data about the following individuals:

- Employees,
- Clients/Customers,
- Suppliers/Service Providers, and
- other individuals whether related directly or indirectly.

(together hereinafter referred to as 'Data Subject/s')

This Data Protection Policy sets out how the Company seeks to protect relevant personal data and moreover how we ensure that our employees and/or service providers appointed by ourselves understand the rules governing personal data to which they have access in the course of their work or in the course of their engagement.

Moreover, this Data Protection Policy requires the employees to ensure that the Board of Directors, and/or the Senior Management, and/or Data Protection Officer (DPO) be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed. The Company encourages all employees to request confirmation from Senior Management and/or the DPO in case of any queries they may have when it comes to processing and/or storing away personal data.

This Data Protection Policy is prepared in line with the Data Protection Act (Chapter 440 of the Laws of Malta), the General Data Protection Regulation (Regulation EU 2016/679 of the European Parliament and of the Council dated 27th April 2016) and any other applicable regulation issued by local authorities.

2. Definitions

The following definitions shall apply without prejudice to the definitions given by the GDP Regulation, by the Data Protection Act (Chapter 440 of the Laws of Malta) and any other applicable rules and regulations. Moreover, these definitions shall apply where relevant and in the context of the Company and its business operations.

Business purposes	The purposes for which personal data may be used by us: Administrative, payroll, payment of dividends or invoices, assignment of rights, and for business development purposes. *Business purposes include the following:* *- Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or request's* *- Ensuring business policies are adhered to (such as policies covering email and internet use);* *-Operational and Administrative reasons,* *- Managing complaints,* *- Monitoring staff conduct, disciplinary matters (in the context of the Employer-Employee relationship),* *- Marketing our business,* *- Improving our services.*
Personal data	Information relating to identifiable individuals, such as clients, customers, service providers, suppliers, current and former employees, job applicant, agencies, and other staff, and marketing contacts.

	Personal data we gather may include: name and surname of individuals, identification number (both local and international), contact details (which could include mobile phone, telephone and/or email address), educational background, financial and pay details, details of certificates and diplomas, details of licences applicable to the Company's business, education and skills, marital status, nationality, job title, and Curriculum Vitaes.
Sensitive personal data	*Personal data about an individual's criminal offences, or related proceedings or any use of sensitive personal data is strictly controlled in accordance with this policy.*

3. Scope

This policy applies to all employees of the Company irrespective to seniority. We encourage all employees to be familiar with this Data Protection Policy and comply with its terms.
This policy supplements our other policies as communicated from time to time.
We may supplement or amend this Data Protection Policy by additional policies and/or internal guidelines from time to time. Any new or modified policy will be circulated to the employees before being adopted.

4. Who is responsible for this policy?

It is our Data Protection Officer, Kira Curmi who may be contacted on kira.curmi@hili.company that has overall responsibility for the day-to-day implementation of this policy. However, in all cases, Senior Management may be consulted by any employee if a query and/or request for data information arises.
In line with this clause, the Company reserves the right to request third-party legal assistance when it comes to specific requests for processing or for any other requests by clients, customers, employees and any other Data Subject.
The policy of the Company is to process personal data fairly and lawfully in accordance with the rights available to all individuals, which rights are made available by the GDPR but which shall be without prejudice to any other rights available to any other individual pursuant to any other relevant law and/or regulation.
Generally speaking we shall not process personal data unless the individual whose details we are processing has consented to this happening, whether directly or indirectly.

5. The responsibilities of the Data Protection Officer and/or of Senior Management within the Company shall be the following**:**
   - Reviewing all data protection procedures and policies on a regular basis;
   - Keeping the board of directors updated about data protection responsibilities, risks and issues;
   - Addressing queries on data protection from employees, board members and other stakeholders within the Company;
   - Addressing queries on data protection from clients/customers, suppliers, service providers and relevant entities or authorities;
   - Reviewing contracts, agreements or other arrangements in the context of data collection and data processing;
   - Reviewing IT processes and website contents in the context of GDPR;
   - Ensure all systems, services, software and equipment meet acceptable security standards;

- Reviewing policies, terms and conditions of third-party service providers engaged by the Company for data storing and data processing;
- Approving data protection statements forming part of emails and other marketing material both in hard and soft copy;
- Arranging data protection training and advice for all employees and those included in this policy;

The processing of all data by the Company must be:

- Directly or indirectly connected to our Business and to our operational procedures;
- Directly or indirectly connected to your needs and requests in the context of you being a client/customer or service provider;
- Necessary and specific to deliver our services;
- In line with the right of any individual's privacy and confidentiality;
- In line with the Data Protection Act of Malta, the GDPR or any other relevant regulation issued by relevant authorities from time to time.

In view of the introduction of the GDPR, the Company has endeavoured to prepare and circulate to the clients and/or customers a Notice of Consent in line with GDPR (hereinafter the 'Notice').

This Notice:

- Sets out the purposes for which we hold personal data on customers and the relationship with the Company;
- Highlights that our work may require us to give information to third parties such as expert witnesses and other professional advisers;
- Provides that customers have a right of access to the personal data that the Company holds about them;
- Contains an 'exit clause' in case the client/customer requests to retrieve the consent being given.

6. Sensitive personal data

In most cases where we process sensitive personal data the Company shall endeavor to obtain the explicit consent of the client, customer or data subject unless exceptional circumstances apply, or unless we are required to process such by any relevant law and/or regulation. 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.
This specific consent letter shall also apply to employees of the Company when the Company is requested to provide such sensitive personal data.

7. Accuracy and relevance

We will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unrelated purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.
Individuals may ask that we correct inaccurate personal data relating to them. The Company encourages any client, customer, employee and/or service provider to approach us should any information that we hold is inaccurate by emailing the DPO on info@mfplc.com.mt.

8. Your personal data

You must take reasonable steps to ensure that personal data we hold about you is accurate and updated from time to time, as required. For example, if your personal circumstances change, please inform the DPO on kira.curmi@hili.company or any other officer of the Company on info@mfplc.com.mt so that they can update your records.

9. Data security

The Company endeavors to keep personal data secure against loss, misuse or destruction thereof. In the context of where we engage third party organizations to process personal data on our behalf, the DPO or any other senior management will establish what, if any, additional specific data security arrangements need to be implemented in the contracts or arrangements with those third-party organizations. It is to be noted however that the responsibility for the data storage and data protection shall remain of the Company even in the context of such being delegated to other third-party organisations.

10. Storing data securely

In cases when data is printed and stored away in hard copies, the Company shall keep such in a secure place where only authorised personnel (as recorded by the Board of Directors from time to time) can access it.
When no longer needed, and also in line with the principle of the 'right to be forgotten', printed hard copy data shall be shredded by the Company.
Any data which is stored electronically on any server, computer or by the use of cloud systems shall be protected by strong passwords that are changed regularly by our IT Department/IT Administrator. We encourage all employees to periodically create, amend and store away their passwords.
Any cloud system or storage media shall be approved by the Board of Directors or the DPO. The servers that contain personal data of clients, customers, employees and service providers shall be kept in a secure location within the premises of the Company or elsewhere as agreed to by the Board of Directors from time to time. These servers are being backed up internally and in line with the IT Policy of the Company. The servers that contain sensitive data shall have approved and protected security software and strong firewall. The IT Administrator in conjunction with the DPO shall be responsible to review such security systems from time to time.
Data stored on CDs or memory sticks must be locked away securely when they are not being used.
The Company does not allow any employee or service provider engaged by the Company to store any personal data directly to mobile devices such as laptops, tablets or smartphones unless such devices are controlled by secured passwords.

11. Data retention

The Company endeavors to retain personal data on any data subject for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into consideration the reasons why the personal data was obtained, but shall in all cases be determined in a manner consistent with our data retention guidelines. The employee, at the termination of his/her engagement with the Company, may request that the personal data is removed and/or destroyed. Likewise, any client, customer or third-party provider may request the Company to delete and/or remove all data pertaining to itself.

12. Transferring data internationally

The forum encapsulated by the GDPR is the European Union Member States and therefore all employees of the Company may not transfer personal data anywhere within the EU without first consulting the Data Protection Officer or a member of the Senior Management.
The Company has taken the position that even though the GDPR applies to European Union member States, all employees of the Company may not transfer personal data internationally outside the EU without first consulting the Data Protection Officer or a member of the Senior Management.

13. Subject access requests

All employees of the Company shall have a right to request from the Company information on the data being held about them. Likewise, clients, customers and/or service providers are entitled to request the Company what information is being held about them or about their company which they have a beneficial interest in.
However, no employee of the Company shall provide information on another employee or on one particular client or customer or service provider unless this is accepted by the DPO or, in exceptional cases, by one of the members of Senior Management in writing.
If an employee receives a subject access request, the employee should refer that request immediately to the DPO.
Please contact the DPO if you would like to correct or request information that we hold about you. There might also be restrictions on the information to which you are entitled to receive under applicable law.

14. Processing data in accordance with the individual's rights

Employees, client, customers and/or service providers might request the Company not to use their personal data for direct marketing purposes. All employees, clients, customers and/or service providers are encouraged to contact the DPO about such request.
Unless a business relationship already exists and the client or customer has already consented to information and marketing material, all employees are precluded from sending direct marketing material to someone electronically (e.g. via email).
Please contact the DPO for advice on direct marketing before starting any new direct marketing activity.

15. Training

The Company endeavours to provide training about this Data Protection Policy to all employees. Moreover, ongoing training may be provided whenever there is a substantial change in the relevant laws or our policies and procedures.
Training to be provided will cover, amongst other things:

- The law relating to data protection under Maltese Law;
- The GDPR and any changes thereafter;
- Our data protection and related policies and procedures.

The Company reserves the right to appoint third party professionals to provide such training.

16. GDPR provisions to apply

Where not specified previously within this policy, the following provisions will be effective as at the 25th May 2018 onwards.

17. Privacy Notice - transparency of data protection

Being transparent and providing accessible information to individuals about how we will use their personal data is important for our organisation. The following are the questions the Company asks itself when collecting data and what we do with such:

What information is being collected?	
Who is collecting it?	
How is it collected?	
Why is it being collected?	
How will it be used?	
Who will it be shared with?	
Identity and contact details of any data controllers	
Details of transfers to third country and safeguards	
Retention period	

18. Conditions for processing

The Company shall ensure that any use of personal data is justified using at least one of the conditions for processing and this will be specifically documented. All staff who are responsible for processing personal data shall be aware of the conditions for processing.

19. Justification for personal data

Any personal data that shall be processed by the Company will be in compliance with all the data protection principles and envisaged by the GDPR and, where applicable, in line with any other principles as emanating from relevant authorities.
The Company shall document any additional justification for the processing of sensitive data and shall ensure that any biometric and genetic data is considered sensitive and processed only after specific consent is gathered by the Company.

20. Consent

The personal data that we collect shall be subject to an active consent by the data subject providing such information and data. This consent can be revoked by the data subject at any time by contacting the DPO on info@mfplc.com.mt.

21. Criminal record checks

The Company may be obliged to conduct due diligence on any data subject, particularly in the fields of Anti-Money Laundering and Terrorist Financing which are 'Criminal' in nature. Any criminal record checks are justified by relevant law and therefore the Company shall have a right to request information from reputable authorities on any data subject in light of the Anti-Money Laundering regulation of other criminal laws.

22. Data portability

Upon request, a client, customers, service provider, an employee, or any data subject shall have the right to receive a copy of their data in a structured format. These requests should be processed within two (2) weeks, provided there is no undue burden and provided it does not compromise the privacy of other individuals. A data subject may also request that their data is transferred directly to another system.

23. Right to be forgotten

A client, customers, service provider, employee or any data subject may request that any information held by the Company relating to them is deleted or removed, and any third parties who process or use that data must also comply with such requests. An erasure request may only be refused by the Company if an exemption based on applicable laws, apply.

24. Privacy by design and default

'Privacy by design' is an approach to projects that promote privacy and data protection compliance from the initial stages or any relationship. The DPO shall be responsible for conducting Privacy Impact Assessments, where necessary, and shall ensure that all IT projects of the Company commence with a privacy plan.
By default, when relevant and when it does not have a negative impact on the data subject, privacy settings will be set to the optimum level of privacy and confidentiality.

25. Data audit and register

The Company may provide inhouse regular data audits to manage and mitigate risks which shall include information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant. Such audits shall be recorded and stored away.

26. Reporting breaches

All employees shall have an obligation to report actual or potential data protection compliance failures. Amongst other things, this will allow the Company to:

- Investigate the failure and take remedial steps if necessary;
- Maintain a register of compliance failures;
- Notify the relevant authority of any compliance failures that are material either in their own right or as part of a pattern of failures.

27. Monitoring

All employees shall be obliged to observe this policy. The DPO has overall responsibility for this policy and he/she shall monitor it regularly to make sure it is being adhered to.

28. Consequences of Non-Compliance

The Company takes compliance with this data protection policy very seriously. Failure to comply in a strict manner shall put you and the organisation at risk.
Any failure by any employee to comply with this data protection policy may lead to disciplinary action and, in exceptional cases, may lead in dismissal.
We encourage all employees that should they have any questions or concerns about the contents of this data protection policy, they should contact the DPO or any other member of Senior Management.