Marvelsoft Ltd. Hong Kong

DATA PROTECTION POLICY

This policy sets out how our organisation protects personal data

1 Document Contents Page

2 Document Version Control

	Last Modified	Last Modified By	Document Changes
0.1	Obfuscated	Obfuscated	Initial document text entry and creation
0.2	Obfuscated	Obfuscated	Modifications of text
0.3	Obfuscated	Obfuscated	Adding paragraphs explaining how we implement requirements
0.4	Obfuscated	Obfuscated	Modifications to the policy
0.5	Obfuscated	Obfuscated	Addtional modifications of policy articles
1.0	Obfuscated	Obfuscated	Approval for publishing

3 Data Protection Policy

3.1 Purpose

The purpose of this policy is to comply with company and regulatory requirements, in particular under the Hong Kong Personal Data Privacy Ordinance (the “PDPO”) and the EU GDPR and to protect the rights of data subjects in their personal data.

Marvelsoft adheres to applicable laws, respects the privacy rights, and is strongly committed to process personal information with high integrity. It uses reasonable technical and organisational measures to ensure the integrity, completeness and adequacy of personal information.

3.2 Scope

All employees and third-party users.

Personal Data as defined by the PDPO and GDPR.

3.3 Principle

Personal data is classified and treated as classification level Confidential, and all associated policies, controls and processes apply.

3.4 Data Protection Policy Statement

The company is classed as a Data Controller/Data Processor based on the context of the processes under the current PDPO and GDPR. This policy confirms our commitment to protect the privacy of the personal information of our customers, clients, employees, and other interested parties. We have engaged in a programme of Information Security Management which is aligned to the international standard ISO 27001 to ensure that the processes of personal information are conducted using best practice processes.

4 Legal Basis for Processing

Article 6 of the GDPR provides the legal basis under which Personal Data can be processed. Our legal basis for processing is documented in our Record of Processing Activities.

During the recruitment process, individuals applying for a job have to provide personal information to Marvelsoft, who at the same time, usually processes this information in order to assess the merits of the candidate. All candidates must give consent before any screening of the employee may take place.

Further, Marvelsoft processes personal information about its own employees. The personal information collected about the employees is necessary for the employment relationship. Collected information includes, but is not limited to, the employee's name, address, payroll and tax information, contact information of contact person in case of emergency, medical information that is crucial to absence data because of illness, and performance reviews. Marvelsoft does not share employee information with third parties except if it is necessary for the performance of its contractual and employment obligations. It may for example share information with authorities or organisations in charge of pensions to ensure pensions are paid or with social security or health organisations to ensure that benefits are awarded and contributions made.

Employees are encouraged to contact human resources for more specific information on what information is collected.

Marvelsoft collects professional contact information of representatives of customers and suppliers and processes this information in order to implement its contractual relationship with such. Marvelsoft may use such information in the performance of its contractual obligations and to provide services. It does not share such information with third parties except if it is necessary for the performance of its contractual obligations. Marvelsoft does not have access to any personal information collected by the customer or the supplier themselves, such as information of their customers and employees. In fact, the customer or supplier information collected is limited to information that is relevant and necessary for the customer or supplier relationship.

Marvelsoft may collect personal information from users through Marvelsoft's website if individuals provide information voluntarily (such as users name, e-mail, address or telephone number). Any personal information submitted through our website is used by Marvelsoft to provide support or services that the individual has requested. Moreover, Marvelsoft does not use cookies except for those that are essential for its website to function.

5 Data protection principles

The company is committed to processing data in accordance with its responsibilities under the General Data Protection Regulation (GDPR) and PDPO. Article 5 of the GDPR requires that personal data shall be collected and processed in accordance with the following principles.

5.1 Lawfulness, Fairness and Transparency

Personal data is processed lawfully, fairly and in a transparent manner in relation to individuals.
We review and document the data that we control and or process and make the determination of the legal basis for processing. We provide privacy notice by publishing this policy on our website and thus inform data subjects of their rights as well as what processing takes place, by whom, for how long and why. Should processing change we would update this policy and publish the updated version on our website.

5.2 Purpose Limitation

Personal data is collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is possible and not be incompatible with the initial purposes.
We ensure we only process data for the purposes for which it has been collected and communicated and not for other reasons without the agreement and knowledge of the Data Subject(s) as indicated above under Article 4.

5.3 Data Minimisation

The personal data collected or processed should be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed. We ensure that data collected is not excessive and is appropriate to the purpose for which it was collected. We conduct Data Privacy Impact Assessments as part of our project lifecycle.
We minimise the collection of personal user data, limited to user name, user professional email address and user phone number.

5.4 Accuracy

Data collected and processed should be accurate and kept up to date; Marvesoft takes reasonable steps to ensure that personal data that are inaccurate, having regard to the

purposes for which they are processed, are erased, or rectified. We rely on customers, suppliers, users and employees to provide accurate data and check accuracy whenever is possible, and allow for rectification or erasure if needed.

5.5 Storage Period Limitation

Personal data kept for no longer than is necessary for the purposes for which it is processed. Personal data may be stored for longer periods insofar as the personal data will be
processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.
We have implemented a data retention policy and data retention schedule in line with legal, regulatory and company needs. The default retention period for telemetry and metrics is two months. Default retention period for other application related data and logs containing personal data is three months.
The data is automatically deleted at the end of these periods.
Employee data and customer and supplier data are kept for the duration of the relationship and for a period of seven years thereafter to meet legal and tax requirements. A review of stored data is performed once a year and documented.

Personal data is processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.
We have implemented an information security management system in line with ISO 27001 the International Standard for Information Security. We have a culture of information security and assess security controls and requirements throughout the project life cycle.

5.6 Integrity and Confidentiality

Personal Data shall be processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful processing, and against accidental loss, modification, destruction or damage. Marvelsoft shall use appropriate technical and organisational measures to ensure that the integrity and confidentiality of Personal Data is maintained at all times.

5.7 Accountability

The Data Controller shall be responsible for and be able to demonstrate compliance. This means that Marvelsoft must demonstrate that the six Data Protection Principles (outlined above) are met for all Personal Data for which it is responsible.

On top of this Marvelsoft ensures that it complies with the principle of data protection by design. In order to ensure that all aspects of Marvelsoft's business activities comply with personal data protection laws and standards, the definition of new projects, processes, systems and procedures as well as the review of existing processes, systems and procedures shall be subject to review and validation by the data protection team ("DPT"). Each manager at Marvelsoft shall ensure that a data protection impact assessment and action plan is conducted for any and all new and revised projects, processes, systems and/or procedures that can involve the processing of personal data and that are under its responsibility. Such review shall be submitted to and validated by the DPT.

6 Personal Information Classification and Handling

Personal data classification and handling is in line with the Information Classification and Handling Policy.

7 Personal Information Retention

Personal data is retained and destroyed in line with the Information Classification and Handling Policy, Asset Management Policy, and the Data Retention Schedule.

Personal data from our client is kept as outlined above under section 5.5.

Personal data from Marvelsofts' employees are deleted after 10 years.

8 Personal Information Transfers / Transmissions

Personal data is transferred in line with the appropriate level of security and company processes.

Personal information may be transferred between Marvelsoft and its subsidiaries or affiliated companies. All affiliated companies are contractually bound to comply with applicable laws and this policy when processing personal information. EU standard contractual clauses are entered into between such companies to ensure that data is protected in the same way across the board. Further, affiliates abide by this same Data Protection Policy.
Personal information may also be shared with subcontractors that process information on behalf of Marvelsoft.

For example, Marvelsoft has an external payroll administrator that processes personal information of Marvelsoft's employees.
Marvelsoft carefully chooses subcontractors, inter alia, based on information security. All subcontractors are contractually obligated to apply the same degree of protection as Marvelsoft.

9 Personal Information Storage

Personal Information storage is in line with the policies implemented by Marvelsoft as part of its objectives to comply with ISO 27001 standards.

10 Breach

In the event of a breach of the principles of the GDPR and PDPO employees inform their line manager, and /or a member of the Management Review Team and/or Senior Management and follow the pre-arranger incident management process.

Breaches are assessed and where appropriate and required the Data Subjects and / or the relevant authorities are informed without undue delay.

11 The Rights of Data Subjects

Data Subjects have the right to access the personal data, which Marvelsoft has collected relating to them. All Data Subjects have the right to rectify any errors contained in that information. They have a right to portability, restriction of processing and erasure. Prospects and employment candidates who have provided consent have a right to withdraw consent at any time. Marvelsoft employees and employment candidates whose personal data are collected and processed by Marvelsoft based on legitimate interests have a right to object to the collection and processing of their personal data, provided however that Marvelsoft may reject the objection based on compelling legitimate grounds for the processing which override the interests, rights and freedoms of the Data Subject.

The knowledge or consent of the Data Subject on the collection and processing of his personal data is not required in the following situations:

- The prevention, investigation, detection or prosecution of criminal offences.
- The apprehension of offenders.
- The assessment or collection of a tax or duty.
- By court order or by applicable law.

Marvelsoft has set up a Personal Data Protection Team ("DPT") entrusted with the following tasks.
1/ Ensuring compliance by Marvelsoft employees with this policy and applicable personal data protection laws;

2/ Informing Data Subjects of the processing of their personal data and of their rights relating thereto, including the management of notifications;
3/ Coordinating and maintaining records for consent provided, including maintaining a central personal data register;
4/ Providing guidance and advice to various departments relating to personal data protection and related internal processes, including providing training;
5/ Monitoring the implementation of data protection within the Company, preparing data protection impact assessments and drafting and implementing action/remedial plans;
6/ Acting as a contact point for and cooperating with data protection authorities, including making necessary filings with local authorities
7/ Responding to enquiries, objections, and other process requests from Data Subjects;
8/ Carrying out annual personal data protection audits, which will at a minimum assess compliance with this policy, awareness levels and training, and effectiveness of internal processes.

All Data Subjects whose personal information may have been collected by Marvelsoft can contact the Personal Data Protection Team for further information or regarding concerns, requests or questions at dataprotection@marvelsoft.net or by post at marvelsoft's addresses listed at www.marvelsoft.net. Marvelsoft may charge a small fee for extra copying costs (beyond one copy) or a reasonable fee if the request is manifestly unfounded or excessive.
When a Data Subject requests access to his personal data, such data may also contain data pertaining to another individual. In such cases, personal data shall be redacted so that the requesting Data Subject only sees his/her personal data.
The DPT shall endeavour to reply within 30 days of the receipt of a request. The DPT will be able to extend the period of compliance by a further two months where requests are complex or numerous. If this is the case, the DPT must inform the Data Subject within one month of the receipt of the request and explain why the extension is necessary.
The reply may contain, as applicable:

- An acknowledgement of receipt of the request,
- Any information located to date,
- Details of any requested information or modifications which will not be provided to the Data Subject, the reason(s) for the refusal, and any procedures available for appealing the decision,
- An estimated date by which any remaining responses will be provided,
- An estimate of any costs to be paid by the Data Subject (e.g. where the request is excessive in nature),
- The name and contact information of the Marvelsoft employee who the Data Subject should contact for follow up.

For the avoidance of doubt, the DPT is not a Data Protection Officer under the GDPR. Marvelsoft may in the future appoint a Data Protection Officer but is not required by law to do so.

Any incident, deficiency or breach or applicable law relating to personal data protection must be reported to the DPT immediately in order to enable Marvelsoft to identify an appropriate response and meet its legal obligations.

11.1 The right to be informed

Individuals have the right to be informed about how we use their Personal Data.
This includes:

- The name and contact details of our organisation.
- The name and contact details of our representative.
- The contact details of our data protection officer.
- The purposes of the processing.
- The lawful basis for the processing.

11.2 The right of access

- Individuals have the right to access their personal data.
- This is commonly referred to as subject access.
- Individuals can make a subject access request verbally or in writing.
- We have one month to respond to a request unless special circumstances dictate otherwise.
- We generally will not charge a fee to deal in relation to a request.

11.3 The right to rectification

- The GDPR includes a right for individuals to have inaccurate personal data rectified or completed if it is incomplete.
- An individual can make a request for rectification verbally or in writing.
- We have one calendar month to respond to a request.
- In certain circumstances we can refuse a request for rectification.

11.4 The right to erasure (the right to be forgotten)

- The GDPR introduces a right for individuals to have personal data erased.
- The right to erasure is also known as ‘the right to be forgotten’.
- Our clients and individuals can make a request for erasure verbally or in writing.

- We have one month to respond to a request.
- The right is not absolute and only applies in certain circumstances.
- This right is not the only way in which the GDPR places an obligation on us to consider whether to delete personal data.
- Our tool (platform) have the features to respond to data subjects rights requests.

11.5 The right to restrict processing

- Individuals have the right to request the restriction or suppression of their
- personal data.
- This is not an absolute right and only applies in certain circumstances.
- When processing is restricted, we are permitted to store the personal data, but not use it.
- An individual can make a request for restriction verbally or in writing.
- We have one calendar month to respond to a request.

11.6 The right to data Portability

- The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.
- It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting its usability.
- Doing this enables individuals to take advantage of applications and services that can use this data to find them a better deal or help them understand their spending habits.
- The right only applies to information an individual has provided to a controller.

11.7 The right to object

- The GDPR gives individuals the right to object to the processing of their personal data in certain circumstances.
- Individuals have an absolute right to stop their data being used for direct marketing.
- In other cases where the right to object applies, we may be able to continue processing if we can show that we have a compelling reason for doing so.
- We must tell individuals about their right to object.
- An individual can make an objection verbally or in writing.

11.8 Rights in relation to automated decision making and profiling

Individuals have the right not to be subject to a decision when:

- It is based on automated processing, and
- It produces a legal effect or a similarly significant effect on them.

12 Definitions

For the purpose of this policy the following definitions apply:

12.1 Personal Data

Any information relating to an identified or identifiable natural person ("Data Subject") who can be identified, directly or indirectly, 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.

12.2 Sensitive Personal Data

Personal Data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms.
Sensitive Personal Data includes Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, 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.
Marvelsoft does not collect sensitive data.

12.3 Data Controller

The natural or legal person, public authority, agency, or any other body, which alone or jointly with others, determines the purposes and means of the processing of Personal Data.

12.4 Data Processor

A natural or legal person, public authority, agency, or any other body which processes Personal Data on behalf of a Data Controller.

12.5 Processing

An 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 of the data.

12.6 Anonymization

Irreversibly de-identifying Personal Data such that the person cannot be identified by using reasonable time, cost, and technology either by the controller or by any other person to identify that individual. The Personal Data processing principles do not apply to anonymized data as it is no longer Personal Data.

13 Policy Compliance

13.1 Compliance Measurement

The information security management team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal

and external audits, and feedback to the policy owner.

13.2 Exceptions

Any exception to the policy must be approved and recorded by the Information Security Manager in advance and reported to the Management Review Team.

13.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

13.4 Continual Improvement

The policy is updated and reviewed annually as part of the continual improvement process.

14 Marketing

Marvelsoft may contact Customers and/or Prospects and send them promotional or marketing material through digital channels (including mobile phones, email, the internet or any social media) only subject to obtaining the Customer's or Prospect's prior consent except where another legal basis is available such as an existing contractual relationship. No campaign without the Customer's or Prospect's prior consent may be carried out without approval by the DPT. The Prospect shall be informed when first contacted that it has a right to withdraw consent at any time or to opt-out. In case of consent withdrawal, the processing of relevant personal data shall cease immediately and the personal data shall be restricted and kept together with the withdrawal of consent in the Register.

15 Training and Awareness

Marvelsoft employees are hereby informed of their responsibility in ensuring the protection of personal data within the context of their work at Marvelsoft. Additional guidelines and training or awareness campaigns are provided on a regular basis, including at local level when this is warranted by specificities in local regulations.

16 Data breach

Marvelsoft shall report any data breach to the data protection authority at the latest 72 hours after it becomes aware of such breach.

17 Whistleblowing

Any detected breach of personal data protection or weakness in the processes should be reported without delay to the DPT at dataprotection@Marvelsoft.net or by post at the addresses listed under www.marvelsoft.net. The DPT will investigate all claims, even if anonymous, in order to determine whether a data breach has indeed taken place and shall undertake adequate corrective measures.