

Data Protection Policy

Manufacturing Management Malta Limited



Palace Court, Church Street, St Julians STJ 3049 MALTA
625 S. Gay Street, Suite 160, Knoxville TN. 37902 USA

1 Contents

DATA PROTECTION POLICY	4
1 Introduction	4
2 Why this Policy exists	4
3 Definitions.....	4
4 Basic Principles Regarding Personal Data Processing.....	4
i. Lawfulness, Fairness and Transparency	5
ii. Purpose Limitation	5
iii. Data Minimisation	5
iv. Accuracy of Personal Data	5
v. Personal Data Retention	5
vi. Confidentiality.....	5
vii. Accountability	5
viii. Disclosure of Information	6
ix. Cross-border Transfer of Personal Data.....	6
5 Rights of Access by Data Subjects	6
i. Notices to Data Subjects	6
ii. Data Subject’s Consent	6
iii. Fair Processing Guidelines	7
iv. Right to be forgotten	7
v. Data Portability	7
vi. Disposal of Personal Data	7
vii. Security	7
6 The Company’s Responsibilities	7
7 Use of Web Page: www.3-ems.com	8
8 Cookies	8
9 Collection of Data Subject’s Personal Data	8
10 Data Subject’s Support	9
11 Marketing	9
12 Personal Data Breach Incidents	9
13 Audit and Accountability	9

14 Governing Law..... 9

15 Personal Data Protection Contact..... 9

16 Changes to this Policy 9

17 Validity 9

DATA PROTECTION POLICY

1 Introduction

MANUFACTURING MANAGEMENT MALTA LIMITED (hereinafter referred to as the "Company") shall endeavour in complying with the applicable laws related to the General Data Protection Regulation (GDPR 2016/679) in countries where the Company operates.

This Policy sets forth the basic principles by which the Company collects, retains, transfers, discloses and disposes the Personal Data of consumers, customers, suppliers, business partners, employees, users, visitors to the website and other individuals (hereinafter referred to as the "Data Subjects"), and indicates the responsibilities of its business departments and employees while Processing Personal Data.

This Policy applies to the Company and any future subsidiary companies whether directly or indirectly controlled within the European Union (EU) and European Economic Area (EEA) or Processing Personal Data of Data Subjects within the EU and EEA.

The Company has no intention of transferring data outside of the EU and EEA. However, it ensures that in the event that any Personal Data of Data Subjects is transferred outside of the EU and EEA countries or an international organisation in the course of its business, that the legal regime is deemed to provide an "adequate" level of Personal Data protection as stipulated by the European Commission or has provided appropriate safeguards or under binding corporate rules.

The Company warrants that all Personal Data of the customers of its services shall be processed under the applicable regulations governing the protection of Personal Data (GDPR 2016/679).

Personal Data is processed only when there is a legal basis for such an act: legal obligation, contractual relationship, and user consent, protection of key user interests or legitimate interest of the Company.

2 Why this Policy exists

This data protection policy ensures Manufacturing Management Malta Limited:

- Complies with data protection law and follows good practice.
- Protects the rights of employees, customers and partners.
- Is open about how it stores and processes individuals' data.
- Protects itself from the risk of a data breach.

3 Definitions

The following terms "**Controller**", "**Processor**", "**Data Subject**", "**Personal Data**", "**Processing Activity/ies**", "**Pseudonymisation**", "**Cross-Border of Personal Data**", "**Cross-Border Data Transfer Procedure**", "**Supervisory Authority**" used in this document shall have the same meaning as in the European Union's General Data Protection Regulation.

4 Basic Principles Regarding Personal Data Processing

The Company shall adhere to Article 5(2) of the GDPR, which stipulates "the Controller shall be responsible for, and be able to demonstrate, compliance with the principles."

Personal Data must:

1. Be processed fairly and lawfully;
2. Be obtained only for specific, lawful purposes;
3. Be adequate, relevant and not excessive;
4. Be accurate and kept up to date;

5. Not be held for any longer than necessary;
6. Be protected in appropriate ways;

And the Company must:

7. Be Accountable;
8. Disclose information;
9. Not to transfer Personal Data outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection.
10. Process Data in accordance with the rights of Data Subjects;

i. Lawfulness, Fairness and Transparency

The Company shall ensure that the Personal Data in relation to Data Subjects is processed lawfully, fairly and in a transparent manner.

ii. Purpose Limitation

The Company shall collect Personal Data for specified, explicit and legitimate purposes and will not further process Personal Data in a manner that is incompatible with those purposes. Further Processing for archiving purposes in the public interest, scientific or historical research or statistical purposes shall not be deemed incompatible with the initial purposes.

iii. Data Minimisation

The Company shall keep Personal Data that is adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed. The Company shall apply anonymization or Pseudonymisation to Personal Data where possible to reduce the risks to the Data Subjects.

iv. Accuracy of Personal Data

The Company strives to keep Personal Data accurate, and, where necessary, is to be kept up to date. The Company shall take reasonable steps to ensure that Personal Data is accurate, having regard to the purposes for which it is processed, and any inaccurate Personal Data shall be erased or rectified without undue delay.

v. Personal Data Retention

The Company warrants that the Personal Data will not be kept for longer than is necessary and only kept for the purposes for which it is processed. Retention periods may vary from a few months in relation to enquiries to over ten years under applicable law or court orders. The Company stores Personal Data in an electronic password protected remote server and ensures that only principals of the Company have access to such Personal Data. The Company may hold hard copy data for works in progress and ensures adequate locked storage systems in the executive office.

vi. Confidentiality

Taking into account the state of technology and other available security measures, the implementation cost, and likelihood and severity of Personal Data risks, the Company endeavours to use appropriate technical or organizational measures to process Personal Data in a manner that ensures appropriate security of Personal Data, including protection against accidental or unlawful destruction, loss, alternation, unauthorized access to, or disclosure.

vii. Accountability

The Company shall be responsible for and be able to demonstrate compliance with the principles outlined above.

viii. Disclosure of Information

In the event that the Company uses a third-party supplier or business partner to process Personal Data on its behalf, the Company shall ensure that this Processor will provide security measures to safeguard Personal Data that is appropriate to the associated risks.

The Company shall endeavour that the supplier or business partner is to provide the same level of data protection. The Company shall ensure that the supplier or business partner shall process Personal Data only to carry out its contractual obligations towards the Company or upon the instructions of the Company and not for any other purposes.

When the Company processes Personal Data jointly with an independent third party, the Company will explicitly specify its respective responsibilities of and the third party in the relevant contract or any other legal binding document, such as the Supplier Data Processing Agreement.

ix. Cross-border Transfer of Personal Data

The Company shall ensure that before transferring Personal Data out of the European Economic Area (EEA), adequate safeguards will be used including but not limited to the signing of a Data Transfer Agreement/Addendum, as required by the European Union. Authorisation may be obtained from the relevant Data Protection Authority where required. Furthermore, the entity receiving the Personal Data shall comply with the principles of Personal Data Processing set forth in Cross-Border Data Transfer Procedure.

5 Rights of Access by Data Subjects

The Company acting as Data Controller shall provide Data Subjects with a reasonable access mechanism to enable the same to access their Personal Data. The Data Subject shall be allowed to update, rectify, erase, or transmit their Personal Data, if appropriate or as required by law.

i. Notices to Data Subjects

At the time of collection or before collecting Personal Data for any kind of Processing Activities including but not limited to selling products, services, or marketing activities, the Company shall inform the Data Subjects of the following:

- the types of Personal Data collected;
- the purposes of the Processing and the Processing methods;
- the Data Subjects' rights with respect to their Personal Data;
- the retention period including any potential international data transfers;
- if data will be shared with third parties; and
- the Company's security measures to protect Personal Data.

This information shall be provided through a Privacy Notice. All Data Subjects, regardless of the type and legal basis of Processing, may file a complaint against Personal Data Processing to this email address: info@3-ems.com

Where Personal Data is being transferred to a third country, the Privacy Notice should reflect this and clearly state to where, and to which entity Personal Data is being transferred.

ii. Data Subject's Consent

The Company shall ensure that whenever Personal Data is processed, such Processing is carried out based on the Data Subject's consent, or other lawful grounds. The Company shall retain record of such consent.

The Company shall provide Data Subjects with different options to provide their consent and must inform and ensure that their consent (apart from whenever consent is used as the lawful ground for Processing) can be withdrawn at any time.

iii. Fair Processing Guidelines

Personal Data will only be processed when explicitly authorised by the Company. It is in the Company's remit to decide whether to perform the Data Protection Impact Assessment (DPIA) for each data Processing activity following the Data Protection Impact Assessment Guidelines.

iv. Right to be forgotten

Upon request, Data Subjects have the right to have their Personal Data erased by the Company. The Company acting as a Controller will take all necessary actions (including technical measures) to inform any third-party Data Processors where applicable to comply with the request.

v. Data Portability

Data Subjects have the right to receive, upon request, a copy of the Personal Data they provided to the Company in a structured, commonly used and machine-readable format and to transmit such Data to another Controller, for free. The Company shall endeavour to ensure that such requests are processed within one month, subject that it is not excessive and does not affect the rights of other individuals' Personal Data.

vi. Disposal of Personal Data

When the Company receives requests to dispose of Personal Data records by Data Subjects, The Company shall ensure that these requests are handled within a reasonable time frame. The Company shall keep record including a log of these requests.

The Company ensures that any archived Personal Data is disposed of by adequate disposal mechanisms on expiry of retention period. Any hard copies of Personal Data that the Company might have obtained from Data Subjects shall be physically destroyed when no longer relevant. The Company shall also strive in obtaining adequate disposal mechanisms to ensure no Personal Data is leaked outside of the organisation.

vii. Security

The Company shall maintain the accuracy, confidentiality and relevance of Personal Data based on the Processing purpose. The Company shall ensure that adequate security mechanisms designed to protect Personal Data will be used to prevent Personal Data from being stolen, misused or abused, and to prevent Personal Data breaches.

The Company shall be responsible for the requirements in this section and that any present and future collection, retention, transfer, disclosure and disposal methods are compliant with relevant law, good practices and industry standards.

6 The Company's Responsibilities

The Company shall ensure appropriate Personal Data Processing from all its employees and all those who have access and process data on behalf of the Company.

Everyone who works for or with the Company has some responsibility for ensuring that Personal Data is collected, stored and handled appropriately. Each team that handles Personal Data must ensure that it is handled and processed in line with this Policy and data protection principles.

However, these people have key areas of responsibility:

- **The board of directors** is ultimately responsible for ensuring that the Company meets its legal obligations.

- **The IT Manager, is responsible for:**

1. Keeping the board updated about data protection responsibilities, risks and issues;
2. Reviewing all data protection training and advice for the people covered by this Policy;
3. Arranging data protection training and advice or the people covered by this Policy;
4. Handling data protection questions from staff and anyone else covered by this Policy;
5. Dealing with requests from individuals to see the data the Company holds about them (also called 'subjects access requests' [SAR]);
6. Checking and approving any contracts or agreements with third parties that may handle the Company's sensitive data.
7. Ensuring all systems, services and equipment used for storing data meet acceptable security standards;
8. Performing regular checks and scans to ensure security hardware and software is functioning properly;
9. Evaluating any third-party services the Company is considered using to store or process data. For instance, cloud computing services.

- **The Marketing Manager, is responsible for:**

10. Approving any data protection statements attached to communications such as emails and letters;
11. Addressing any data protection queries from journalists or media outlets like newspapers;
12. Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.
13. Personal Data collected

7 Use of Web Page: www.3-ems.com

The Company collects information from the visitors and users of the website in order to better understand the needs of users and to improve their products and services.

The following data is collected for the above stated purposes:

- Time and date of the page visit
- Visited pages
- Type and version of the Internet browser
- Visitor's IP address.

8 Cookies

The Company uses cookies to provide visitors and/or users with full functionality and high-quality content. Cookies are small text files uploaded to visitors' computers with the purpose of tracking the use of certain pages. If accepting cookies option is turned off on the visitor's and/or user's computer, the visitor and/or user can still use the pages, but the functionality of the service will be partially restricted.

9 Collection of Data Subject's Personal Data

The Company may collect personal identification information from Data Subjects in a variety of ways, including, but not limited to, when Data Subjects visit our site.

Data Subjects may be asked for, as appropriate, name, email address, mailing address, phone number. Data Subjects may, however, visit the website anonymously. The Company will collect personal identification information from Data Subjects only if they voluntarily submit such information to the Company. Data Subjects can always refuse to supply personally identification information, except that it may prevent them from engaging in certain website related activities.

10 Data Subject's Support

The Company shall provide its users with user support through an email. The data collected in this manner shall be processed exclusively for the purpose of providing user support.

11 Marketing

The Company, in compliance with the given consent, may periodically notify Data Subjects of the new benefits of The Company. The Data Subject may always decide to decline from receiving the above notifications and may cancel the service by sending an e-mail to: sales@3-ems.com Response to

12 Personal Data Breach Incidents

When the Company learns of a suspected or actual Personal Data breach, the Company shall perform an internal investigation and take appropriate remedial measures in a timely manner. Where there is any risk to the rights and freedoms of Data Subjects, the Company will notify the relevant Supervisory Authorities without undue delay and, when possible, within 72 hours from when it learns of such breach.

13 Audit and Accountability

The administration department or other relevant department is responsible for auditing how well business departments implement this Policy.

Any employee who violates this Policy will be subject to disciplinary action and the employee may also be subject to civil or criminal liabilities if his or her conduct violates laws or regulations.

14 Governing Law

This Policy is intended to comply with the laws and regulations in the place of establishment and of the country in which the Company operates. In the event of any conflict between this Policy and applicable laws and regulations, the latter shall prevail.

15 Personal Data Protection Contact

Requests, complaints or inquiries relating to Processing and protection of Personal Data can be sent to the e-mail address: info@3-ems.com or by calling: +356 2010 3020

In accordance with the applicable legal regulations governing the protection of Personal Data, each request/inquiry will be resolved without undue delay and at the latest within 30 days of receipt.

When contacting and posting such requests, we will invest reasonable efforts to confirm your identity and to prevent unauthorized Personal Data Processing.

16 Changes to this Policy

As the Company evolves, there may be the need to update this Policy to keep pace with changes to the website, software, services, business and Applicable Laws. The Company will however, always maintain its commitment to respect the Data Subject's privacy. The Company ensures that it will notify the Data Subjects with any material changes under this Policy by email (the most recent email provided by the Data Subject) or post any other revisions to this Policy along with their effective date, in an easy-to-find area of the website.

17 Validity

This document was updated on 3rd July 2018 and is effective from that date.

Contact: Robert Ward

Email: Robert.ward@3-ems.com

Company Address: Palace Court, Church Street St Julian's STJ 3049 MALTA