CREATING THE RIGHT ENVIRONMENT

MICHAEL J LONSDALE

FOR INTERNAL USE ONLY

MICHAEL J LONSDALE LTD

DATA PROTECTION POLICY

1. ABOUT THIS POLICY

1.1 This Data Protection Policy sets out how Michael J Lonsdale Ltd ("we", "our", "us", "the Company") obtain, handle, process, transfer and store personal data of our prospective and current customers, suppliers, employees, workers and other third parties that we communicate with.

1.2 This policy sets out rules on data protection and the legal conditions that must be satisfied when we obtain, handle, process, transfer and store personal data.

1.3 We recognise that the correct and lawful treatment of Personal Data will maintain confidence in the organisation and will provide for successful business operations. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times. The Company is exposed to potential fines of up to EUR20 million (approximately £18 million) or 4% of total worldwide annual turnover, whichever is higher and depending on the breach, for failure to comply with the provisions of the GDPR.

1.4 This policy forms part of any employee's contract of employment. You **must** read this policy very carefully and abide by its terms. Failure to adhere to this policy may result in disciplinary action.

1.5 The Data Protection Compliance Manager is responsible for ensuring compliance with the Act and with this policy. That post is held by Arthur Lander, Group Health, Safety and Environmental Director, Arthur.Lander@michaellonsdale.com. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Data Protection Compliance Manager.

2. DEFINITION OF DATA PROTECTION TERMS

Data is information which is stored electronically, on a computer, or in certain paper-based filing systems.

Data controllers are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with the Act. We are the data controller of all personal data used in our business for our own commercial purposes.

Data processors include any person or organisation that is not a data user that processes personal data on our behalf and on our instructions. Employees of data

controllers are excluded from this definition but it could include suppliers which handle personal data on our behalf.

Data subjects for the purpose of this policy include all living individuals about whom we holds personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.

Data users are those of our employees whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times.

Explicit Consent: consent which requires a very clear and specific statement (that is, not just action).

Personal Data means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (for example, a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour. Personal Data includes Sensitive Personal Data.

Personal Data Breach: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

Privacy Notices or Privacy Policies: separate notices setting out information that may be provided to Data Subjects when the Company collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or the website privacy policy) or they may be stand-alone, one time privacy statements covering Processing related to a specific purpose.

Processing or Process is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

Pseudonymisation or Pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

Sensitive personal data information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal Data relating to criminal offences and convictions.

Sub-Contractor Privacy Policy: our policy in providing its customers, suppliers and other third parties detailed and specific information required by the GDPR to identify the legal grounds being relied on by the Company for each Processing activity.

3. SCOPE

3.1 Everyone has rights with regard to the way in which their data is handled. During the course of our activities we will collect, store and process personal data and sensitive personal data about our contractors, suppliers and other third parties, and we recognise that the correct and lawful treatment of this data will maintain confidence in the organisation and will provide for successful business operations.

3.2 Data users are obliged to comply with this policy when processing personal data on our behalf. Any breach of this policy may result in disciplinary action.

4. DATA PROTECTION PRINCIPLES

4.1 We adhere to the principles relating to Processing of Personal Data set out in the GDPR which require Personal Data to be:

(a) Processed lawfully, fairly and in a transparent manner (Fair and Lawful Processing).

(b) Collected only for specified, explicit and legitimate purposes (Purpose Limitation).

(c) Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation).

(d) Accurate and where necessary kept up to date (Accuracy).

(e) Not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (Storage Limitation).

(f) Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful

Processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality).

(g) Not transferred to another country without appropriate safeguards being in place (Transfer Limitation).

(h) Made available to Data Subjects and Data Subjects allowed to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests).

4.2 We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability).

5. FAIR AND LAWFUL PROCESSING

5.1 Personal data must be processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

5.2 You may only collect, process and share Personal Data fairly and lawfully and for specified purposes. The GDPR restricts our actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent Processing, but ensure that we process Personal Data fairly and without adversely affecting the Data Subject.

5.3 The GDPR allows Processing for specific purposes, some of which are set out below:

(a) the Data Subject has given his or her Consent (see section 14);

(b) as identified in our Third Party Privacy Policy (processing is necessary for the performance of a contract, to meet our legal compliance obligations, to protect the Data Subject's vital interests, to pursue our legitimate interest).

5.4 Our Third Party Privacy Policy will allow you to identify and document the legal ground being relied on for each Processing activity.

6. PURPOSE LIMITATION

6.1 Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further Processed in any manner incompatible with those purposes.

6.2 You cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless you have informed the Data Subject of the new purposes and they have Consented where necessary.

7. DATA MINIMISATION

7.1 Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed.

7.2 You may only Process Personal Data when performing your job duties requires it. You cannot Process Personal Data for any reason unrelated to your job duties.

7.3 You may only collect Personal Data that you require for your job duties: do not collect excessive data. Ensure any Personal Data collected is adequate and relevant for the intended purposes.

7.4 You must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with the Company's data retention policy.

8. ACCURACY

8.1 Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

8.2 You must ensure that the Personal Data that we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. You must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards.

8.3 If you believe that Personal Data that we use is not accurate, complete, kept up to date or relevant for the purpose for which we collected it, you must notify the Data Protection Compliance Manager without delay.

9. STORAGE LIMITATION

9.1 Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

9.2 The Company will maintain retention policies and procedures to ensure Personal Data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires such data to be kept for a minimum time. You must comply with our data retention policy.

9.3 All Personal Data or Sensitive Personal Data must be stored and processed through our hosted and secure database Mitrefinch. You must not store Personal Data or Sensitive Personal Data on any personal devices, USBs or other personal equipment unless such devices are password protected and that such passwords are updated regularly.

10. SECURITY INTEGRITY AND CONFIDENTIALITY

10.1 Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.

10.2 We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data (including use of encryption and Pseudonymisation where applicable).

10.3 We will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

(a) **Confidentiality** means that only people who are authorised to use the data can access it.

(b) **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed.

(c) **Availability** means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on the Michael J Lonsdale Ltd central computer system instead of individual PCs.

10.4 Security procedures include:

(a) **Entry controls.** Any stranger seen in entry-controlled areas should be reported.

(b) **Secure lockable desks and cupboards.** Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)

(c) **Methods of disposal.** Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required.

(d) **Equipment.** Data users must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

10.5 You must follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. You may only transfer Personal Data to third-party service providers who agree to

comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

10.6 You must comply with and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with the GDPR and relevant standards to protect Personal Data.

11. TRANSFER LIMITATION

11.1 The GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined. You transfer Personal Data originating in one country across borders when you transmit, send, view or access that data in or to a different country.

11.2 You must not transfer Personal Data outside the EEA without the Data Protection Compliance Manager's written consent.

12. DATA SUBJECT'S RIGHTS AND REQUESTS

12.1 Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

(a) withdraw Consent to Processing at any time;

(b) receive certain information about the Data Controller's Processing activities;

(c) request access to their Personal Data that we hold;

(d) prevent our use of their Personal Data for direct marketing purposes;

(e) ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;

(f) restrict Processing in specific circumstances;

(g) challenge Processing which has been justified on the basis of our legitimate interests or in the public interest;

(h) request a copy of an agreement under which Personal Data is transferred outside of the EEA;

(i) object to decisions based solely on Automated Processing, including profiling (ADM);

(j) prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;

(k) be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;

(l) make a complaint to the supervisory authority; and

(m) in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine readable format.

12.2 You must verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you into disclosing Personal Data without proper authorisation).

12.3 You must immediately forward any Data Subject request you receive to the the Data Protection Compliance Manager who will thereafter deal with the subject access request.

13. ACCOUNTABILITY

13.1 As a Data Controller, we have implemented appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. As Data Controller, we are responsible for, and must be able to demonstrate, compliance with the data protection principles.

14. CONSENT – APPLIES TO EMPLOYEES AND SUB-CONTRACTORS

14.1 We, as Data Controller, must only process Personal Data on the basis of one or more of the lawful bases set out in the GDPR, which include Consent.

14.2 If you deal with recruitment employees or staffing at sites, you **MUST** provide such personnel with our Site Induction Checklist and Consent Notice. You must ensure that such personnel signs and returns the Site Induction Checklist and Consent Notice before such personnel enters into or works within a construction site. If such personnel refuse to sign the Consent Notice, you must notify Data Protection Compliance Manager immediately.

14.3 Data Subjects are able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured. If a Data Subject confirms that they wish to withdraw their consent, immediately notify our Data Protection Compliance Manager.

15. TRANSPARENCY (NOTIFYING DATA SUBJECTS)

15.1 The GDPR requires Data Controllers to provide detailed, specific information to Data Subjects depending on whether the information was collected directly from Data S**u**bjects or from elsewhere. Therefore, before we engage with a sub-contractor to undertake work on a project, you **MUST** draw the Data Subject's (sub-contractor's) attention to the Sub-Contractor Privacy Policy published on our website.

15.2 Whenever you deal with recruitment and collect Personal Data directly from employees or workers, including for human resources or employment purposes, at the point you collect such Personal Data you must provide the Data Subject with our Employee Privacy Policy.

15.3 Such privacy notices will provide the information required by the GDPR including our identity as Data Controller, how and why we will use, Process, disclose, protect and retain that Personal Data which must be presented when the Data Subject first provides the Personal Data.

16. REPORTING A PERSONAL DATA BREACH

16.1 The GDPR requires Data Controllers to notify any Personal Data Breach to the applicable regulator and, in certain instances, the Data Subject.

16.2 We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where we are legally required to do so.

16.3 If you know or suspect that a Personal Data Breach has occurred, **DO NOT** attempt to investigate the matter yourself. Immediately contact the Data Protection Compliance Manager who is designated as the key point of contact for Personal Data Breaches. You should preserve all evidence relating to the potential Personal Data Breach and immediately report this to the Data Protection Compliance Manager.

17. TRAINING AND AUDIT

17.1 We will ensure that all Company Personnel have undergone adequate training to enable them to comply with data privacy laws.

17.2 You must undergo all mandatory data privacy related training as requested.

17.3 You must regularly review all the systems and processes under your control to ensure they comply with this Privacy Standard and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

18. SHARING PERSONAL DATA

18.1 Generally we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

18.2 You may only share the Personal Data we hold with another employee, agent or representative of the company if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.

18.3 You may only share the Personal Data we hold with third parties, such as our service providers if:

(a) they have a need to know the information for the purposes of providing the contracted services;

(b) sharing the Personal Data complies with the Customer Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;

(c) the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;

(d) the transfer complies with any applicable cross border transfer restrictions; and;

(e) a fully executed written contract that contains GDPR approved third party clauses has been obtained.

19. DEALING WITH SUBJECT ACCESS REQUESTS

19.1 Data subjects can make a formal request for information we hold about them. This must be made in writing. Employees who receive a written request should forward it to the Data Protection Compliance Manager immediately.

19.2 When receiving telephone enquiries, you will only disclose personal data we hold on our systems if the following conditions are met:

(a) you check the caller's identity to make sure that information is only given to a person who is entitled to it.

(b) you suggest that the caller put their request in writing if we are not sure about the caller’s identity and where their identity cannot be checked.

19.3 Our employees will refer a request to their line manager or the Data Protection Compliance Manager for assistance in difficult situations. Employees should not be bullied into disclosing personal information.

20. CHANGES TO THIS POLICY

We reserve the right to change this policy at any time. Where appropriate, we will notify data subjects of those changes by mail or email.

Acknowledgement of receipt and review

I, [EMPLOYEE NAME], acknowledge that on [DATE], I received and read a copy of Michael J Lonsdale Ltd's Data Protection Policy and understand that I am responsible for knowing and abiding by its terms.

I understand that the information in the Data Protection Policy is intended to help company personnel work together effectively on assigned job responsibilities and assist in the use and protection of personal data.

Signed …….

Name …….

Dated …….