LODGE SECURITY

DATA PROTECTION POLICY

CONTENTS **Page**

1. OBJECTIVE

Lodge Service are committed to being transparent about how it collects and uses the personal data of its employees and to meeting its data protection obligations under the General Data Protection Regulations (GDPR). This policy sets out our commitment to data protection, individual rights and obligations in relation to the personal data of job applicants, employees, workers, contractors, volunteers, interns, apprentices and former employees (company personnel) referred to as 'personal data'. This policy does not apply to the personal data of clients, members or other personal data processed for business purposes.

2. SCOPE

This Data Protection Policy applies to all Personal Data we process regardless of the media on which the data is stored or whether it relates to past or present job applicants, employees, workers, contractors, volunteers, interns, apprentices and former employees.

This Data Protection Policy applies to all Company Personnel. You must read, understand and comply with this Data Protection Policy when processing Personal Data on our behalf and attend training on its requirements. This Data Protection Policy sets out what we expect from you in order for the Company to comply with applicable law. Your compliance with this Data Protection Policy is mandatory. Any breach of this Data Protection Policy may result in disciplinary action.

Personal Data processed in relation to clients, members of other personal data processed for business purposed will be processed in accordance with agreements in place.

This Data Protection Policy is an internal document and should not be shared with third parties, clients, members or regulators without prior authorisation from the Data Protection Officer (DPO) or Data Protection Representative.

We have appointed Ametros Group Ltd as the Data Protection Officer (DPO). The Group People Director is the Data Protection Representative with responsibility for data protection compliance within the Company. Please contact the

Group People Director with any questions about the operation of this Data Protection Policy or if you have any concerns that this Data Protection Policy is not being, or has not been, followed.

will sometimes be referred to as , “we” or “us”.

3. PRINCIPLES

We process personal data in accordance with the following data protection principles:-

- Processing personal data lawfully, fairly and in a transparent manner;
- Collecting personal data only for specified, explicit and legitimate purposes;
- Processing personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing;
- Keeping accurate personal data and taking all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay;
- Retaining personal data only for the period necessary for processing;
- Adopting appropriate measures to make sure that personal data is secure and protected against unauthorised or unlawful processing and accidental loss, destruction or damage;
- Ensuring that personal data is not transferred to another country without appropriate safeguards being in place and;
- Ensuring that personal data is made available to Data Subjects and that the Data Subjects are allowed to exercise certain rights in relation to their Personal Data.

All Company Personnel are responsible for and must be able to demonstrate compliance with the data protection principles listed above.

4. DEFINITIONS

"Personal Data" is any information that relates to a living individual who can be identified from that information. Processing is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.

"Special categories of personal data" means information about:-

- An individual’s racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs, or other beliefs of a similar nature;
- Trade Union membership;
- Health;
- Sexual life or sexual orientation;
- Biometric data;

5. BASIS FOR PROCESSING

We set out the reasons for processing personal data, how we use such data and the legal basis for processing in our Privacy Notice. We will not process personal data of individuals for other reasons. Where we rely on legitimate interests as the basis for processing data, we will carry out an assessment to ensure that those interests are not overridden by the rights and freedoms of individuals.

We will update personal data promptly if an individual advises that their information has changed or is inaccurate.

Personal data gathered during the employment, volunteer relationship, or apprenticeship or internship will be held in the employees personnel file in hard copy and electronic format. The periods for which the Company holds personal data are contained in our Privacy Notice.

We will maintain a record of our processing activities in respect of personal data in accordance with the requirements of the General Data Protection Regulation (GDPR).

6. DATA SECURITY

We take the security of personal data seriously and have internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure and to ensure that data is not accessed, except by employees in the proper performance of their duties.

We will ensure that personal information about you, including information in personnel files, is securely retained. We will keep hard copies of information in a locked filing cabinet. Information stored electronically will be subject to access controls and passwords and encryption software will be used where necessary.

Where laptops (or any other similar electronic (or otherwise) devices) are taken off site, you must follow any relevant policies relating to the security of information and the use of computers for working at home/bringing your own device to work.

7. DATA BREACHES

If we discover that there has been a breach of personal data that poses a risk to the rights and freedoms of employees, we will report this to the Information Commissioner within 72 hours of discovery. We will record all data breaches regardless of their effect.

If the breach is likely to result in a high risk to the rights and freedoms of employees, we will inform the affected employees that there has been a breach and provide them with information about its likely consequences and the mitigation measures we have taken.

If you become aware of an actual or suspected data breach you must immediately inform the Data Protection Representative and DPO (dpo@ametrosgroup.com) providing full details of the breach or suspected breach.

8. INDIVDIAUL RESPONIBILITES

Employees are responsible for helping the Company keep their personal data up-to-date. You should let the Company know if data that you have provided changes, for example, if you move house or change bank details.

You may also have access to the personal data of other individuals and of our clients and members in the course of your employment. Where this is the case, the Company relies on individuals to help meet its data protection obligations to employees, clients and members. If you acquire any personal information in the course of your duties, you must ensure that it is treated in accordance with the principles set out in Section 3.

In particular, you should ensure that you:-

- Only access data that they have authority to access and only for authorised purposes;
- Do not disclose data except to individuals (whether inside or outside the Company) who have appropriate authorisation;
- Keep data secure (for example by complying with rules on access to premises, computer access, including password protection and secure file storage and destruction);

- Do not remove personal data, or devices containing or can be used to access personal data, from the Company's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device;
- Do not store personal data on local drives or on personal devices which are used for work purposes and;
- Do not remove any personal data from our premises, save in circumstances where you have obtained the prior consent of you manager, DPO, Data Protection Representative.

If you acquire any personal information in error by whatever means, you should inform the Data Protection Representative immediately and, if it is not necessary for you to retain that information, arrange for it to be handled by the appropriate individual within the organisation.
Where you are required to disclose personal data to any other country, you must ensure first that there are adequate safeguards for the protection of data in the host country. For further guidance on the transfer of personal data outside the UK speak to the Data Protection Representative.

If you are in any doubt about what you may, or may not do with personal information, you should seek advice from the Data Protection Representative or DPO, if you are unable to do so immediately you should not disclose the information concerned.

9. INDIVIDUAL RIGHTS

As an employee and Data Subject, you have a number of rights in relation to your personal data and have the right to make a Subject Access Request (SAR).

If you wish to make a SAR, we will advise you:-

- Whether or not your data is processed and if it is, the categories of personal data concerned and the source of the data if it is not collected from you directly;
- To whom your personal data is or may be disclosed, including any recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers;
- For how long your personal data is stored (or how that period is decided);
- Your rights to rectification or erasure of data, or to restrict or object to processing;
- Your right to complain to the Information Commissioners Office (ICO) if you think the Company has failed to comply with your data protection rights; and
- Whether or not we carry out automated decision-making and the logic involved in any such decision-making. We will also provide you with a copy of the personal data undergoing processing.

We will normally respond to a request within a period of one month from the date it is received. In some cases, such as where we process large amounts of your data, we may respond within three months of the date the request is received, where this may be the case, we will advise you in writing within one month of receiving your original request.

If a subject access request is manifestly unfounded or excessive, the Company is not obliged to comply with it. Alternatively, we can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A SAR is likely to be manifestly unfounded or excessive where it repeats a request to which the Company has already responded. If an individual submits a request that is unfounded or excessive, we will notify them that this is the case and whether or not we will respond to it.

10. CORRECTION, UPDATING AND DELETION OF DATA

You have a number of other rights in relation to the personal data that we hold and can ask the Company to:-

- Rectify inaccurate data;
- Stop processing or erase data that is no longer necessary for the purposes of processing;
- Stop processing or erase data if your individual interests override the Company's legitimate grounds for processing data (where the Company relies on its legitimate interests as a reason for processing data);
- Stop processing or erase data if processing is unlawful; and
- Stop processing data for a period if data is inaccurate or if there is a dispute about whether or not your individual interests override the Company's legitimate grounds for processing data.

To ask the Company to take any of these steps, you should notify the Data Protection Representative immediately and provide any necessary corrections and/or updates to the information.

11. TRANSFER OF PERSONAL DATA OUTSIDE THE EEA

We will not transfer your personal data to any country outside the European Economic Area (EEA) other than those that have been granted an adequacy decision under the General Data Protection Regulation (GDPR).

We may be required to transfer your personal data to organisations who intend to transfer the data outside the EU. Where such transfers of data take place, we shall ensure that contracts are in place between the parties involved that ensure the recipient organisation has a suitable standard of data protection in place.

12. CONSEQUENCES OF NON-COMPLIANCE

All employees are under an obligation to ensure that they have regard to the principles set out in Section 3 when accessing, using or disposing of personal information.

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under the Company's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee, client or members data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

Failure to observe these data protection principles may also constitute a criminal offence and result in an employee incurring personal criminal liability.

13. REVIEW OF PROCEDURES AND TRAINING

We will provide training to all employees on data protection matters during their induction and on a regular basis thereafter. If you consider that you would benefit from refresher training, you should contact you manager.

Employees whose roles require regular access to personal data, or who are responsible for implementing this policy, or responding to subject access requests under this policy will receive additional training to help them to understand their duties and how to comply with them.

We will review and ensure legal compliance with this policy and procedure on a regular basis and reserve the right to make reasonable changes, amendments or variations to this Policy.