Data Protection Policy

Newline Logic Limited ('the Company'), trading as Daracore, is fully committed to full compliance with the requirements of the Data Protection Act 1998 and The EU General Data Protection Regulation (GDPR). The Company will therefore follow procedures which aim to ensure that all employees, contractors, consultants, partners or other servants or agents of the Company (collectively known as data users) who have access to any personal data held by or on behalf of the Company are fully aware of and abide by their duties under the Data Protection Act 1998 and GDPR.

1. Statement of Policy:

The Company needs to collect and use information about people with whom it works in order to operate and carry out its functions.

These may include members of the public, current, past and prospective employees, clients, customers and suppliers. In addition, the Company may be required by law to collect and use information in order to comply with the requirements of central government. This personal information must be handled and dealt with properly however it is collected, recorded and used and whether it is on paper, in computer records or recorded by other means.

The Company regards the lawful and appropriate treatment of personal information as very important to its successful operations and essential to maintaining confidence between the Company and those with whom it carries out business. The Company therefore fully endorses and adheres to the Principles of the Data Protection Act 1998 and GDPR.

The Company will maintain a 'Certificate of Registration' with the Information Commissioners Office (ICO) at all times and will ensure the content is current and valid.

2. Handling Personal / Sensitive Data:

The Company will, through management and use of appropriate controls, monitoring and review:

- Obtain explicit consent, in an intelligible and easily accessible form, with the purpose of data processing attached to that consent
- Use personal data in the most efficient and effective way to deliver better services
- Strive to collect and process only the data or information which is needed
- Use personal data for such purposes as are described at the point of collection, or for purposes which are legally permitted
- Strive to ensure information is accurate
- Not keep information for longer than is necessary
- Securely destroy data which is no longer needed
- Implement appropriate technical and organisational measures to safeguard information (including unauthorised or unlawful processing and accidental loss or damage of data). Privacy by design, not addition.
- Ensure that information is not transferred abroad without suitable safeguards
- Ensure that there is general information to employees / candidates of their rights to access information
- Ensure that the Company has an officer specifically responsible for data protection in the Company
- Provide guidance and training for staff at an appropriate level
- Ensure that any breaches of this policy are dealt with appropriately
- Ensure that the rights of people about whom information is held can be fully exercised, these rights include:
    a. The right to access their own personal information within 40 days of request, and when in electronic form, free of charge
    b. The right to prevent processing in certain circumstances
    c. The right to correct, rectify, block or erase information regarded as wrong information
    d. The right to be forgotten - The data subject has a right to have the data controller erase his / her personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data. The conditions for erasure, as outlined in article 17, include the data no longer being relevant to original purposes for processing, or a data subject withdrawing consent.

3. The Principles of Data Protection

The Data Protection Act stipulates that anyone processing personal data must comply with 8 principles of good practice. These principles are legally enforceable.

Summarised, the principles require that personal data:

1. Shall be processed fairly and lawfully and in particular, shall not be processed unless specific conditions are met
2. Shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes
3. Shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed
4. Shall be accurate and where necessary, kept up to date
5. Shall not be kept for longer than is necessary for that purpose or those purposes
6. Shall be processed in accordance with the rights of data subjects under the Act
7. Shall be kept secure, i.e. protected by an appropriate degree of security
8. Shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection

The Act provides conditions for the processing of any personal data. It also makes a distinction between personal data and 'sensitive' personal data.

Personal data is defined as data relating to a living individual who can be identified from:

- Any information related to a natural person or 'Data Subject', that can be used to directly or indirectly identify the person.
- It can be anything from a name, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer IP address.

Sensitive personal data is defined as personal data consisting of information as to:

- Racial or ethnic origin
- Political opinion
- Religious or other beliefs
- Trade union membership
- Physical or mental health or condition
- Sexual life / orientation
- Criminal proceedings or convictions

Authorised by the Directors, for and on behalf of Newline Logic Limited, trading as Daracore:

Signed:

Kevin Hodgers

Director

March 2020