General Data Protection Regulations
Policy 021

This policy applies to:

- Oracle Care Ltd;
- All staff operating on behalf of Oracle Care Ltd

This policy is operational from **25 May 2018.**

The purpose of this policy is to enable Oracle Care Ltd to:

- Comply with our legal, regulatory and corporate governance obligations and good practice
- Gather information as part of investigations by regulatory bodies or in connection with legal proceedings or requests
- Ensure business policies are adhered to (such as policies covering email and internet use)
- Fulfill operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of commercially sensitive information, security vetting, credit scoring and checking
- Investigate complaints
- Check references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments
- Monitor staff conduct, disciplinary matters
- Market our business
- Improve services

This policy applies to information relating to identifiable individuals e.g. staff, applicants, former staff, clients, suppliers and other third party contacts.

Oracle Care Ltd will:

- Comply with both the law and good practice
- Respect individuals' rights
- Be open and honest with individuals whose data is held
- Provide training and support for staff who handle personal data, so that they can act confidently and consistently

Oracle Care Ltd recognises that its first priority under the GDPR is to avoid causing harm to individuals. In the main this means:

- Complying with your rights,
- Keeping you informed about the data we hold, why we hold it and what we are doing with it,
- Keeping information securely in the right hands, and
- Holding good quality information.

Secondly, GDPR aims to ensure that the legitimate concerns of individuals about the ways in which their data may be used are taken into account. In addition to being open and transparent, Oracle Care Ltd will seek to give individuals as much choice as is possible and reasonable over what data is held and how it is used. This includes the right to erasure where data is no longer necessary and the right to rectification where the data is incorrect. Full details are available in the Privacy Notice issued at the point of gathering the data.

Oracle Care Ltd has identified the following potential key risks, which this policy is designed to address:

- Breach of confidentiality (information being given out inappropriately).
- Insufficient clarity about the range of uses to which data will be put — leading to Data Subjects being insufficiently informed
- Failure to offer choice about data use when appropriate
- Breach of security by allowing unauthorised access
- Failure to establish efficient systems of managing changes, leading to personal data being not up to date
- Harm to individuals if personal data is not up to date
- Insufficient clarity about the way personal data is being used e.g. given out to general public
- Failure to offer choices about use of contact details for staff, clients workers or employees.

In order to address these concerns, to accompany this policy, we have an accompanying Information Security Policy 047 and we will issue the Employee Privacy Notices to explain what data we have, why we have it and what we will do with it. The Employee Privacy Notice 048 will also explain the data subjects rights. We will offer training to staff where this is necessary and appropriate in the circumstances to ensure compliance with GDPR. Such training will vary according to the role, responsibilities and seniority of those being trained.

We aim to keep data only for so long as is necessary which will vary from according to the circumstances.

We have no intention to transfer data internationally.

The person responsible for Data Protection is currently our GDPR Officer - Carmine Bianco, Finance Director, with the following responsibilities:

- Briefing the board on Data Protection responsibilities
- Reviewing Data Protection and related policies
- Advising other staff on Data Protection issues
- Ensuring that Data Protection induction and training takes place
- Notification
- Handling subject access requests

- Approving unusual or controversial disclosures of personal data
- Approving contracts with Data Processors
- Ensuring Data is stored securely
- Maintain a Data Audit and keep this up to date
- Reporting breaches to the Information Commissioners Office and the relevant Data Subject(s)

Significant breaches of this policy will be handled under Carmine Bianco, Finance Director, disciplinary procedures which may amount to gross misconduct.

Subject Access Request

Any subject access requests will be handled by the GDPR Officer

Subject access requests must be in writing. All staff are required to pass on anything, which might be a subject access request to the GDPR Officer without delay. The applicant will be given their data within 1 month unless there are complexities in the case which justify extending this to 2 months. You will be notified of any extensions to the deadline for response and the reasons as soon as possible.

We have the right to refuse a subject access request where data is requested at unreasonable intervals, manifestly unfounded or excessive. You will be notified of the reasons as soon as possible.

Where the individual making a subject access request is not personally known to the GDPR Officer their identity will be verified before handing over any information.

The required information will be provided in a permanent and portable form unless the applicant makes a specific request to be given supervised access in person.

You have the right to request the information we hold is rectified if it is inaccurate or incomplete. You should contact the GDPR Officer and provide with the details of any inaccurate or incomplete data. We will then ensure that this is amended within one month. We may, in complex cases, extend this period to two months.

You have the right to erasure in the form of deletion or removal of personal data where there is no compelling reason for its continued processing. We have the right to refuse to erase data where this is necessary in the right of freedom of expression and information, to comply with a legal obligation for the performance of a public interest task, exercise of an official authority, for public health purposes in the public interest, for archiving purposes in the public interest, scientific research,

historical research, statistical purposes or the exercise or defence of legal claims. You will be advised of the grounds of our refusal should any such request be refused.

GDPR Officer is Carmine Bianco – Financial Director

Issued: 25th May 2018
Review: As legislation requires