GDRP Policy

INTRODUCTION

The Company is committed to being transparent about how it collects and uses Personal Data, and to meeting its data protection obligations. This policy sets out the Company's commitment to data protection, and individual rights and obligations in relation to Personal Data and should be read in conjunction to the Privacy Notice/s issued.
To aid understanding of this policy:

- **A Data Controller** is a person or Company that determines when, why and how to Process Personal Data. As a Data Controller the Company is responsible for establishing practices and policies in line with Data Protection Legislation. We are the Data Controller of all Personal Data relating to our Company Personnel and Personal Data used in our business for our own commercial purposes; and

- **Special Category** means: any data set which includes details or reveals race or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, generic data, biometric data, data concerning health, sex, sexual orientation or sex life.

DEFINITIONS

For the purposes of this policy the following definitions are applicable:

- **Company Personnel**: all employees, workers (including contractors, agency workers and consultants), directors, members and others (including volunteers, interns and apprentices);

- **Data Subject**: a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data. This could be you, your colleagues, customers and suppliers or indeed any other person.

- **Data Protection Legislation**: the General Data Protection Regulations EU 2016/679 (GDPR) and all applicable regulations, domestic legislation and any successor legislation relating to the protection of individuals with regards to the processing of personal data to which the Company [and each relevant Group Company] is subject;

- **Personal Data**: any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access, including but not limited to, data held in a filing system. Personal Data includes Special Categories of Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal Data can be factual (for example,

a name, email address, location or date of birth) or an opinion about that person's actions or behaviour. This could include information in an electronic, paper or other format (e.g. images, multimedia, etc.);

- **Personal Data Breach**: any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of Personal Data.

- **Privacy Notices (also referred to as Fair Processing 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; and

- **Processing or Process**: any activity that involves the use of Personal 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 transmitting or transferring Personal Data to third parties.

WHAT AND WHO DOES THIS POLICY APPLY TO?

This Policy applies to all Personal Data we Process regardless of the media on which that data is stored or whether it relates to past or present employees, workers, customers, clients or supplier contacts, shareholders, website users or any other Data Subject.

This policy applies to all Company Personnel ("you", "your"). You must read, understand and comply with this Policy when Processing Personal Data on our behalf and attend training on its requirements. This Policy sets out what we expect from you in order for the Company to comply with applicable law. Any breach of this Policy may result in disciplinary action.

HOW WILL THE COMPANY PROCESS PERSONAL DATA?

The Company will process Personal Data in accordance with the following data protection principles:

- the Company will Process Personal Data lawfully, fairly and in a transparent manner.
- the Company will collect Personal Data only for specified, explicit and legitimate purposes.
- the Company will Process Personal Data only where it is adequate, relevant and limited to what is necessary for the purposes of Processing.
- the Company will keep accurate Personal Data and takes all reasonable steps to ensure that inaccurate Personal Data is rectified or deleted without delay.
- the Company will keep Personal Data only for the period necessary for Processing; and

- the Company will adopt appropriate measures to make sure that Personal Data is secure, and protected against unauthorised or unlawful Processing, and accidental loss, destruction or damage.

The Company will tell individuals the reasons for Processing their personal data, how it uses such data and the legal basis for Processing in its Privacy Notices. It will not Process Personal Data of individuals for other reasons.

The Company will update Personal Data promptly if an employee advises that his/her information has changed or is inaccurate. The employee is under an obligation to keep the Company updated of any changes to their Personal Data.

Personal Data gathered during employment, engagement as a worker, contractor or volunteer, or an apprenticeship or internship, is held in the individual's personnel file (in hard copy or electronic format, or both), and on HR systems. The periods for which the Company holds Personal Data are contained in its Privacy Notices as issued to individuals at the point data is collected, or at other points as the Company deems its obligations require.

WHAT ARE MY OWN RIGHTS, AS A DATA SUBJECT?

As Data Subjects, Company Personnel have several rights in relation to their Personal Data. These are detailed in the relevant Privacy Notice provided to you. If you require a copy of this Privacy Notice, it is available from the HR Manager.

HOW DO I MAKE A DATA SUBJECT ACCESS REQUEST?

Individuals have the right to make a subject access request. If an individual makes a subject access request, the Company will tell him/her:

- whether or not his/her data is Processed and if so why, the categories of Personal Data concerned and the source of the data if it is not collected from the individual.
- to whom his/her data is or may be disclosed, including to recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers.
- for how long his/her Personal Data is stored (or how that period is decided).
- his/her rights to rectification or erasure of data, or to restrict or object to Processing.
- his/her right to complain to the Information Commissioner if he/she thinks the Company has failed to comply with his/her data protection rights; and
- whether or not the Company carries out automated decision-making and the logic involved in any such decision-making.

The Company will also provide the individual with a copy of the Personal Data undergoing Processing. This will normally be in electronic form if the individual has made a request electronically, unless he/she agrees otherwise.

To make a subject access request, the individual should send the HR Manager. In some cases, the Company may need to ask for proof of identification before the request can be Processed. The Company will inform the individual if it needs to verify his/her identity and the documents it requires.

The Company will normally respond to a request within a period of one month from the date it is received. In some exceptional cases, such as where the Company Processes large amounts of the individual's data, it may respond within two months of the date the request is received. The Company will write to the individual within one month of receiving the original request to tell him/her if this is the case.

If a subject access request is manifestly unfounded or excessive, the Company is not obliged to comply with it. Alternatively, the Company may agree to respond but will charge an administrative fee. A subject access request 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, the Company will notify the individual that this is the case and confirm whether or not it will respond to it.

WHAT SHOULD I DO IF I RECEIVE A DATA SUBJECT ACCESS REQUEST, OR IF SOMEONE ASKS ME TO PROVIDE THEIR DATA TO THEM?

You must immediately forward any Data Subject request you receive to the HR Manager and take steps to comply with the above Data Subject response procedure.

HOW SHOULD YOU PROCESS PERSONAL DATA FOR THE COMPANY?

Everyone who works for, or on behalf of, the Company has some responsibility for ensuring data is collected, stored and handled appropriately, in line with this policy and the Company's Data Security and Data Retention policies.

The Company's Data Protection Officer is responsible for reviewing this policy and updating the Board of Directors on the Company's data protection responsibilities and any risks in relation to the Processing of data. You should direct any questions in relation to this policy or data protection to this person.

You should only access Personal Data if you need it for the work you do for, or on behalf of the Company and only if you are authorised to do so. You should only use the data for the specified lawful purpose for which it was obtained.

You should not share Personal Data informally.

You should keep Personal Data secure and not share it with unauthorised people.

You should regularly review and, where required or requested, update Personal Data you deal with. This includes telling us if your own contact details change.

You should not make unnecessary copies of Personal Data and should keep and dispose of any copies securely.

You should use strong passwords and not share your passwords with any other person.

You should lock your computer screens when not at your desk.

Consider anonymising data or using separate keys/codes so that the Data Subject cannot be identified.

Do not save Personal Data to your own personal computers or other devices.

Personal Data should never be transferred outside the European Economic Area except in compliance with the law and authorisation of the HR Manager.

You should lock drawers and filing cabinets. Do not leave paper with Personal Data lying about.
You should not take Personal Data away from Company's premises without authorisation from the HR Manager.

Personal Data should be shredded and disposed of securely when you have finished with it.
You should ask for help from our Data Protection Officer/Data Protection Manager if you are unsure about data protection or if you notice any areas of data protection or security we can improve upon.

Any deliberate or negligent breach of this policy by you may result in disciplinary action being taken against you in accordance with our disciplinary procedure.

It is a criminal offence to conceal or destroy Personal Data which is part of a subject access request (see below). This conduct would also amount to gross misconduct under our disciplinary procedure, which could result in your dismissal.

It should be noted that whilst this list provides examples, this is by no means an exhaustive list and you may be notified of other specific rules from time to time.

WHAT PURPOSES CAN PERSONAL DATA BE PROCESSED FOR?

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.

Personal Data cannot be used 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.

IS THERE A LIMIT TO HOW MUCH PERSONAL DATA CAN BE COLLECTED AND PROCESSED?

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

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.

You may only collect and Process 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.

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 guidelines.

WHAT SHOULD I DO IF PERSONAL DATA IS OUTDATED OR INCORRECT?

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

You must ensure that the Personal Data we use, and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. You must follow the Company's instructions to ensure the accuracy of Personal Data, including instructions related to destroying or amending inaccurate or out-of-date Personal Data.

HOW LONG CAN PERSONAL DATA BE STORED

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

You must not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which we originally collected it, including for the purpose of satisfying any legal, accounting or reporting requirements.

The Company will maintain retention policies and procedures to ensure Personal Data is deleted at the point of no longer being required or the Company having no further lawful purpose for Processing. This is unless a law requires such data to be kept for a minimum time. If you have any queries related to the retention period for Personal Data, please address these to the HR Manager.

PRIVACY BY DESIGN

We are required to implement Privacy by Design measures when Processing Personal Data by implementing appropriate technical and Company measures in an effective manner, to ensure compliance with data privacy principles.

Some of the Processing that the Company carries out may result in risks to privacy. Where Processing would result in a high risk to individual's rights and freedoms, the Company will carry out a data protection impact assessment to determine the necessity and proportionality of Processing.

This will include considering the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks.
How will Personal Data be protected?

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

We will develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of Personal Data that we own or maintain on behalf of others and identified. We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our Processing of Personal Data.

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.

You must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

- **Confidentiality** means that only people who have a need to know and are authorised to use the Personal Data can access it.

- **Integrity** means that Personal Data is accurate and suitable for the purpose for which it is Processed; and

- **Availability** means that authorised users can access the Personal Data when they need it for authorised purposes.

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

WILL I RECEIVE TRAINING ON DATA PROTECTION?

Individuals 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, may receive additional training to help them understand their duties and how to comply with them as appropriate.

At any time, if you have any questions about the operation of this Policy or Data Protection Legislation, not covered in training, please contact the HR Manager.

WHAT SHOULD HAPPEN IN THE EVENT OF A DATA BREACH OCCURRING?

If the Company suspects or discovers that there has been a breach of Personal Data, and that this could pose a risk to the rights and freedoms of individuals, we will report the breach to the Information Commissioner within 72 hours of discovery. The Company will record all data breaches regardless of their effect and employees must therefore report any breach, regardless of any perceived level of severity.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, the Company will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken

If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the person or team designated as the key point of contact for Personal Data Breaches the HR Manager. You should preserve all evidence relating to the potential Personal Data Breach. Failure to notify the designated person or team in itself may result in disciplinary action being taken against you.

WILL THE COMPANY TAKE DISCIPLINARY ACTION IF THERE IS A DATA BREACH?

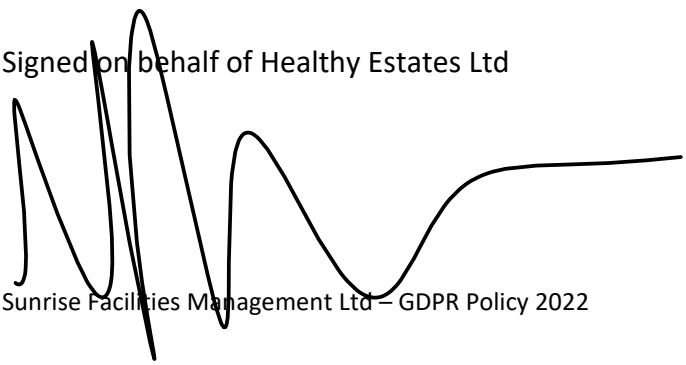
No disciplinary action would automatically be taken simply as a result of a breach having occurred. An investigation would first need to be carried out, to establish the causes of the breach.
Where investigation reveals that a data breach has been caused (wilfully or negligently or without due care and attention) through an employee's actions or inactions, this may lead to disciplinary action being taken. In the event of a serious breach and/or a failure to follow the appropriate procedures the Company has put in place for data Processing, this could amount to an offence of gross misconduct.

Failure to report a breach, or suspected breach, could result in disciplinary action. In serious cases this could amount to an offence of gross misconduct.

CHANGES TO THIS POLICY

We reserve the right to change this policy at any time.

Signed on behalf of Healthy Estates Ltd



Neil Pownall
Director
Jan 2022