

# Data Protection policy & statement

Data protection terms, principles, processing data, notifying data subjects, security, transfer of data, disclosure, sharing and subject access requests.

Everyone has rights with regard to the way in which their personal data is handled.

Whose data we collect;

During the course of our activities we will collect, store and process personal data about our employees, customers, suppliers and other third parties.

The types of personal data that we may be required to handle include information about current, past and prospective customers, service users, employees, suppliers and others that we communicate with.

Our policy

The enclosed Data Protection Policy advises on data protection and the legal conditions that must be satisfied when we obtain, handle, process, transfer and store personal data.

It is subject to certain legal safeguards specified in the combined data protection Laws (UK GDPR and DPA 2018) and other regulations related to personal data.

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.

The enclosed data breach policy has details on detecting and responding to personal data breach occurrences.

Who's responsible for our compliance

The Data Protection Officer is responsible for ensuring our compliance with data protection legislation and with this policy.

If you have any questions about the operation of this policy or any concerns that the policy has not been followed, you can write to:

DPO Enquiries

Rvive

Lake Farm Business Park

Allington Lane

Fair Oak, Hampshire

SO50 7DD

Martin Grainger

Director

## DEFINITION OF DATA PROTECTION TERMS

1.1. Data subjects for the purpose of this policy include all living individuals about whom we hold 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.

1.2. 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, a unique reference number, address or date of birth) or it can be an opinion about that person, their actions and behaviour.

1.3. 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 UK GDPR. Rvive is in most cases the data controller of personal data it collects or uses in its day to day business and in providing services.

1.4. Data processors are any person or organisation that processes personal data on our behalf and on our instructions. Staff of data controllers are not data processors, but it includes suppliers, providers and contractors which handle personal data on Rvive's behalf.

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

1.6. Special Category Data is information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership and genetic data, biometric data (for the purpose of uniquely identifying an individual), data concerning health, an individual's sex life or sexual orientation. Special Category Data can only be processed under strict conditions. Personal Data relating to criminal convictions and offences is subject to additional requirements and should be handled in a similar way to Special Category Data.

1.7. Third Party - Any individual/organisation other than the data subject, the data controller or its processors.

## RESPONSIBILITIES UNDER THE DATA PROTECTION LEGISLATION

2.1. Rvive is a Data Controller of personal information it processes on its own behalf it is also a Processor of information for other organisations. Rvive maintains records of all its processing activities and keeps records of the lawful basis for processing categories of data.

2.2. The Data Protection Officer is responsible for monitoring compliance with the Data Protection Legislation and with this policy and may assign officers to support this process.

2.3. Compliance with Data Protection Legislation is the responsibility of everybody who processes personal information.

## DATA PROTECTION PRINCIPLES

Anyone processing personal data must comply with the six principles relating to processing of personal data in the UK GDPR. These provide that personal data must be:

3.1. Processed lawfully, fairly and in a transparent manner in relation to the data subject

(‘lawfulness, fairness and transparency’). For personal data to be processed lawfully, it must be processed on the basis of one of the lawful bases set out in the UK GDPR. Relevant examples of these bases include, processing that is necessary:

- for the performance of a task carried out in the public interest or in the exercise of official authority vested in Rvive
- for the performance of a contract to which the data subject is party
- for compliance with a legal duty
- the data subject has given consent for the data to be processed for a specific purpose(s). When special category data is being processed, additional conditions must be met. When processing personal data as a data controller in the course of our business, we will ensure that those requirements are met. Personal data is processed in a transparent manner by providing data subjects with privacy notices. These are supplied to the data subject directly and/or are available on Rvive's website.

3.2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. We will only process personal data for the specific purpose(s) set out in Rvive's records and privacy notices or for any other purposes specifically permitted by the legislation. We will notify those purposes to the data subject when we first collect the personal data or as soon as possible thereafter.

3.3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’). Personal data, which is not necessary for the purpose for which it is obtained, should not be collected. If personal data is given or obtained which is excessive for the purpose, it should be deleted or destroyed without delay.

3.4. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘accuracy’). Personal Data, which is kept for a long time, must be reviewed and updated as necessary. No personal data should be kept unless it is reasonable to assume that they are accurate. It is the responsibility of individuals to ensure

that personal data held by Rvive is accurate and up to date. Individuals should notify Rvive of any changes in circumstance or of factual details e.g. change of name or contact details to enable personal records to be updated accordingly. It is the responsibility of Rvive to ensure that any notification regarding change of circumstances is noted and acted upon.

3.5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed ('storage limitation'). We will not keep personal data longer than is necessary for the purpose(s) for which they were collected. We will take all reasonable steps to destroy, or erase from our systems, all data which is no longer required. Data will be kept in accordance with Rvive's retention periods which ensure that data is not kept for longer than necessary.

On occasion, personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) of the UK GDPR.

3.6. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality'). Rvive has appropriate security measures in place to protect data, details of which are provided below. 6.

#### NOTIFYING DATA SUBJECTS

4.1. If we collect personal data directly from data subjects, we will inform them through our Privacy Notices about:

- (a) The purpose or purposes for which we intend to process that personal data.
- (b) The legal basis for processing.
- (c) The types of third parties, if any, with which we will share or to which we will disclose that personal data.
- (d) The length of time that we will retain the data.
- (e) The means, if any, with which data subjects can limit our use and disclosure of their personal data.
- (f) Their right to make a complaint to the ICO.

4.2. If we receive personal data about a data subject from other sources, we will provide the data subject with this information within the required timescales.

4.3. We will also inform data subjects whose personal data we process that we are the data controller with regard to that data, and the contact details of our Data Protection Officer.

#### DATA SECURITY

5.1. We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or destruction of, personal data.

5.2. We will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction.

5.3. Personal data will only be transferred to a data processor who has provided sufficient guarantees to implement appropriate technical and organisational measures that will comply with the Data Protection Legislation and ensure that data subjects rights are protected and that these requirements are governed by a contract or other legally binding agreement.

5.4. 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 personal data should 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 personal data if they need it for authorised purposes.

5.5. Security procedures include:

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

- (b) Secure lockable desks and cupboards. Desks and cupboards will be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)
- (c) Methods of disposal. Paper documents will be shredded and securely disposed of. Digital storage devices will be physically destroyed when they are no longer required.
- (d) Equipment. County Council staff will ensure that the personal data they use in the course of their work is only shared with those who are entitled to see it.
- (e) IT Security. Rvive will maintain up to date firewalls, patching and other IT security measures.

5.6. Training for staff includes:

- (a) Mandatory training for all staff on Data Protection, with refresher training
- (b) Training about data security is provided where required.

5.7. Governance and assurance procedures include:

- (a) An Information Governance framework overseen by the Data Protection Officer
- (b) The regular audit of Rvive's Information Management processes and procedures.

## DISCLOSURE AND SHARING OF PERSONAL INFORMATION

6.1. We will only disclose or share a data subject's personal data where we are legally permitted to do so, in order to comply with any legal obligation, or in order to enforce or apply any contract with the data subject or other agreements; or to protect our rights, property, or safety of our staff, customers, or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.

6.2. Rvive will enter into Data Sharing Agreements with other data controllers where appropriate.

## INDIVIDUAL'S RIGHTS UNDER THE UK GDPR

7.1. Individuals have a number of rights under the UK GDPR including the right to:

- ask Rvive if it holds personal information about them
  - ask what it is used for
  - be given a copy of the information
  - be given details about the purposes for which Rvive uses the information and of other organisations or persons to whom it is disclosed.
  - ask for incorrect data to be corrected.
  - be given a copy of the information with any unintelligible terms explained
  - be given an explanation as to how any automated decisions taken about them have been made.
  - ask that information about them is erased ("right to be forgotten")
  - ask Rvive not to use personal information:
    - o for direct marketing,
    - o to make decisions which significantly affect the individual, based solely on the automatic processing of the data.
- 9.2. Some of these rights are subject to conditions which are set out in the UK GDPR. If Rvive is unable to respond to a request, it will outline the reasons for its decision clearly.

## DEALING WITH DATA SUBJECT RIGHTS REQUESTS

8.1. Rvive has provided application forms on its website to assist data subjects to make a request regarding their personal data.

8.2. Data subjects can make a request for information we hold about them. We recommend that these requests are made in writing where possible. Staff who receive a request should forward it to Rvive's DPO team.

8.3. Any individual who wishes to exercise their data subject rights should on request provide satisfactory proof of identity and sufficient information to enable the data to be located.

8.4. Subject to satisfactory completion of the 8.3 above, Rvive should respond within one month and in accordance with any relevant exemptions specified in the legislation.

## DEALING WITH A POTENTIAL DATA PROTECTION BREACH

9.1. A personal data breach means a breach of security leading to the accidental or unlawful

destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.

9.2. Rvive has a process for managing data protection incidents.

As part of the process staff are required to follow guidelines on reporting a potential data protection breach including completing a data incident reporting form.

#### DATA PROTECTION IMPACT ASSESSMENTS

10.1 Rvive must carry out a Data Protection Impact Assessment (DPIA) when processing personal data is likely to result in a high risk to the rights and freedoms of natural persons. This process identifies and mitigates any potential risks to the rights and freedoms of the data subject prior to new data processing being undertaken.

10.2. Rvive has a procedure for staff to follow which includes guidance on assessing whether a DPIA is required.

#### RETENTION AND DISPOSAL OF DATA

11.1. Rvive discourages the retention of personal data for longer than they are required.

Personal data must be disposed of in a way that protects the rights and privacy of data subjects (e.g., shredding, disposal as confidential waste, secure electronic deletion).

#### FREEDOM OF INFORMATION ACT 2000

13.1 The Freedom of Information Act 2000 (FOIA) allows public access to all types of information held by public authorities. Requests for personal information will be dealt with under the Data Protection Legislation.