



## Rapidata Services Limited – Data Protection Policy May 2018

### 1. Introduction

Rapidata Services Limited (company number: 03311791) (“**Rapidata**”) collects and uses certain types of information about the individuals or service users who come into contact with Rapidata, either directly or through processing data for our clients, in order to carry on our work and provide services. We collect and process the data in accordance with the General Data Protection Regulation (**GDPR**) (EU) 2016/679.

This policy sets out certain principles about how we manage personal data. If we have agreed a bespoke contract that contains conflicting data protection provisions, the terms of that contract will apply instead of this.

### 2. Data Controller

Rapidata is the **data controller** in relation to data that is given directly to us by individuals and organisations. It is also responsible for notifying the Information Commissioner of the data it holds or is likely to hold, and the general purposes that this data will be used for.

For data that we receive and process on behalf of our clients then Rapidata is the **data processor** and we are acting under instruction of and advising the client who is the data controller.

### 3. Disclosure

Rapidata may disclose personal data which it holds to third parties in order to carry out our work.

The individual/service user will be made aware in most circumstances how and with whom their personal data will be shared. There are circumstances where the law allows Rapidata to disclose personal data (including special category data) without the data subject’s consent.

These are:

- carrying out a legal duty or as authorised by the Secretary of State;
- protecting vital interests of an individual/service user or other person;
- the individual/service user has already made the information public;
- conducting any legal proceedings, obtaining legal advice or defending any legal rights;
- monitoring for equal opportunities purposes – i.e. race, disability or religion; and
- providing a confidential service where the individual/service user’s consent cannot be obtained or where it is reasonable to proceed without consent.



Rapidata regards the lawful and correct treatment of personal data as very important to successful working, and to maintaining the confidence of those with whom we deal.

Rapidata intends to ensure that personal data is treated lawfully and correctly.

Rapidata will adhere to the principles of data protection, as detailed in Article 5 of the GDPR.

- a) processed lawfully, fairly and in a transparent manner in relation to individuals;
- b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- d) 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;
- e) 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; 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 subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
- f) 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.”.

Rapidata will, through appropriate management and strict application of criteria and controls:

- observe fully conditions regarding the fair collection and use of personal data;
- meet its legal obligations to specify the purposes for which personal data is intended to be used;



- collect and process personal data only to the extent that it is needed to fulfill its operational needs or to comply with any legal requirements;
- ensure the accuracy of personal data used;
- ensure that the rights of people about whom information is held, can be fully exercised under the GDPR. These include:
  - the right to prevent processing that is likely to cause damage or distress to themselves or anyone else;
  - the right of access to one's personal data held by a data controller;
  - the right to prevent processing for direct-marketing purposes; and
  - the right to correct, rectify, block or erase information which is regarded as wrong information;
- take appropriate technical and organisational security measures to safeguard personal data against unlawful or unauthorized processing of personal data and against the accidental loss of, or damage to, personal data;
- ensure that personal data is not transferred abroad without suitable safeguards;
- treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information; and
- set out clear procedures for responding to requests for information.

#### **4. Data collection**

Informed consent is when an individual/service user clearly understands why their information is needed, who it will be shared with, the possible consequences of them agreeing or refusing the proposed use of their personal data and then gives their consent.

Rapidata will ensure that data is collected within the boundaries defined in this policy. This applies to data that is collected in person, or by completing a form.

When collecting data, Rapidata will ensure that the individual/service user:

- clearly understands why their personal data is needed;
- understands what it will be used for and what the consequences are should the individual/service user decide not to give consent to processing;



- as far as reasonably possible, grants explicit consent, either written or verbal for data to be processed;
- is, as far as reasonably practicable, is competent enough to give consent and has given so freely without any duress; and
- has received sufficient information on why their personal data is needed and how it will be used.

## **5. Data Storage**

Information and records relating to service users will be stored securely and will only be accessible to authorised staff or contractors.

Information will be stored only for as long as it is needed or required by statute and will be disposed of appropriately at the end of such time.

It is Rapidata's responsibility to ensure all personal and company data is non-recoverable from any computer system previously used within the organisation which has been passed on/sold to a third party.

## **6. Data access and accuracy**

All individuals/service users have the right to access the personal data which Rapidata holds about them. Rapidata will take reasonable steps to ensure that this data is kept up to date.

In addition, Rapidata will ensure that:

- its employees processing personal data understand that they are contractually responsible for following good data protection practice;
- its employees processing personal data are appropriately trained to do so and are appropriately supervised;
- anybody wanting to make enquiries about Rapidata's handling of personal data knows what to do;
- it deals promptly and courteously with any enquiries about handling personal data;
- it describes clearly how it handles personal data;
- it will regularly review and audit the ways it stores, manages and uses personal data;
- it regularly assesses and evaluates its methods and performance in relation to handling personal data; and



- all staff are aware that a breach of the rules and procedures identified in this policy may lead to disciplinary action being taken against them.

We reserve the right to change this policy at any time. This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the GDPR.

In case of any queries or questions in relation to this policy please contact  
**Matt Steel, Data Protection Officer**

Signed: Scott Gray

Position: CEO

Date: 25<sup>th</sup> May 2018



## Glossary of Terms

**Data controller** – the person who (either alone or with others) decides what personal data Rapidata will hold and how it will be held or used.

**Individual/service user** – the person whose personal information is being held or processed by Rapidata for example: a client, an employee, or donor.

**Explicit consent** – is a freely given, specific and informed agreement by an individual/service user in the processing of personal data about her/him. Explicit consent is needed for processing special category data.

**Notification** – notifying the Information Commissioner about the data processing activities of Rapidata as certain activities may be exempt from notification.

Information on exemptions can be found on the ICO website: <https://ico.org.uk/for-organisations/guide-to-data-protection/exemptions/>

**Information Commissioner** – the UK Information Commissioner responsible for implementing and overseeing the GDPR.

**Processing** – means any activity that involves the use of data including but not limited to collecting, amending, handling, storing or disclosing personal data.

**Personal data** – data about living individuals that enables them to be identified – e.g. name and address. It does not apply to information about organisations, companies and agencies but applies to named persons, such as individual employees or contractors within the company.

**Special category data** – is personal data which the GDPR says is more sensitive, and so needs more protection:

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life; or
- sexual orientation.