

**Out of Hours Typing Ltd**  
**Data Retention Policy**  
**May 2018**

**1. Introduction**

This Policy sets out the obligations of Out of Hours Typing Ltd, a company registered in the United Kingdom under number 6007030, whose registered office is at 21 Champford Lane, Wellington, Somerset, TA21 8BH (“the Company”) regarding retention of personal data collected, held, and processed by the Company in accordance with EU Regulation 2016/679 General Data Protection Regulation (“GDPR”).

The GDPR defines “personal data” as any information relating to an identified or identifiable natural person (a “data subject”). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

The GDPR also addresses “special category” personal data (also known as “sensitive” personal data). Such data includes, but is not necessarily limited to, data concerning the data subject’s race, ethnicity, politics, religion, trade union membership, genetics, biometrics (if used for ID purposes), health, sex life, or sexual orientation.

Under the GDPR, personal data shall be kept in a form which permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. In certain cases, personal data may be stored for longer periods where that data is to be processed for archiving purposes (subject to the implementation of the appropriate technical and organisational measures required by the GDPR to protect that data).

In addition, the GDPR includes the right to erasure or “the right to be forgotten”. Data subjects have the right to have their personal data erased (and to prevent the processing of that personal data) in the following circumstances:

- a) Where the personal data is no longer required for the purpose for which it was originally collected or processed (see above);
- b) When the data subject withdraws their consent;
- c) When the data subject objects to the processing of their personal data and the Company has no overriding legitimate interest;
- d) When the personal data is processed unlawfully (i.e. in breach of the GDPR);
- e) When the personal data has to be erased to comply with a legal obligation.

This Policy sets out the type(s) of personal data held by the Company, the period(s) for which that personal data is to be retained, the criteria for establishing and reviewing such period(s), and when and how it is to be deleted or otherwise disposed of.

For further information on other aspects of data protection and compliance with the GDPR, please refer to the Company’s Data Protection Policy.

## **2. Aims and Objectives**

- 2.1 The primary aim of this Policy is to set out limits for the retention of personal data and to ensure that those limits, as well as further data subject rights to erasure, are complied with. By extension, this Policy aims to ensure that the Company complies fully with its obligations and the rights of data subjects under the GDPR.
- 2.2 In addition to safeguarding the rights of data subjects under the GDPR, by ensuring that excessive amounts of data are not retained by the Company, this Policy also aims to improve the speed and efficiency of managing data.

## **3. Scope**

- 3.1 This Policy applies to all personal data held by the Company.
- 3.2 Personal data, as held by the Company or third party data processors (the typists) is stored in the following ways and in the following locations:
  - a) The typists engaged by the Data Controller use client-specific template documents during their transcription of audio files. These client-specific templates are not stored on individual typists' computers but rather are worked upon and saved in each typist's One Drive. Each completed document is then uploaded to an individual secure Dropbox folder for each typist and thereafter downloaded and stored on the Company's OneDrive account after returning a copy of each completed item to the Company's client(s).

## **4. Data Subject Rights and Data Integrity**

All personal data held by the Company is held in accordance with the requirements of the GDPR and data subjects' rights thereunder, as set out in the Company's Data Protection Policy.

- 4.1 Data subjects are kept fully informed of their rights, of what personal data the Company holds about them, how that personal data is used, and how long the Company will hold that personal data (usually for the period the data subject is engaged by the Company and thereafter as necessary for HMRC audit purposes).
- 4.2 Data subjects are given control over their personal data held by the Company including the right to have incorrect data rectified, the right to request that their personal data be deleted or otherwise disposed of (notwithstanding the retention periods otherwise set by this Data Retention Policy), and the right to restrict the Company's use of their personal data.

## **5. Technical and Organisational Data Security Measures**

- 5.1 The following technical measures are in place within the Company to protect the security of personal data:
  - a) All emails containing personal data must be encrypted;
  - b) All emails containing personal data must be marked "confidential";
  - c) Personal data may only be transmitted over secure networks;
  - d) Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself and associated temporary files should be deleted;

- e) All hardcopies of personal data, along with any electronic copies stored on physical media should be stored securely;
- f) Personal data must be handled with care at all times and should not be left unattended or on view;
- g) Computers used to view personal data must always be locked before being left unattended;
- h) No personal data should be stored on any mobile device;
- i) All electronic copies of personal data should be stored securely using passwords and encryption;
- j) All passwords used to protect personal data should be changed regularly and should must be secure;
- k) Under no circumstances should any passwords be written down or shared. If a password is forgotten, it must be reset using the applicable method. The Company's IT consultants do not have access to passwords;
- l) All software should be kept up-to-date.

5.2 The following organisational measures are in place within the Company to protect the security of personal data:

- a) All data subjects working on behalf of the Company shall be made fully aware of both their individual responsibilities and the Company's responsibilities under the GDPR and under the Company's Data Protection Policy;
- b) Only parties working on behalf of the Company that need access to, and use of, personal data in order to perform their work shall have access to personal data held by the Company (for example, in the event of an audit by HMRC);
- c) Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;
- d) The performance of those data subjects and other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed;
- e) All parties working on behalf of the Company handling personal data will be bound by contract to comply with the GDPR and the Company's Data Protection Policy;
- f) Where any agent, contractor or other party working on behalf of the Company handling personal data fails in their obligations under the GDPR and/or the Company's Data Protection Policy, that party shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

## 6. Data Disposal

Upon the expiry of the data retention periods set out below in Part 7 of this Policy, or when a data subject exercises their right to have their personal data erased, personal data shall be deleted, destroyed, or otherwise disposed of as follows:

- 6.1 Personal data stored electronically (including any and all backups thereof) shall be deleted securely;
- 6.2 Personal data stored in hardcopy form shall be shredded.

## 7. Data Retention

- 7.1 As stated above, and as required by law, the Company shall not retain any personal data for any longer than is necessary in light of the purpose(s) for which that data is collected, held, and processed.
- 7.2 Different types of personal data, used for different purposes, will necessarily be retained for different periods (and its retention periodically reviewed), as set out below.
- 7.3 When establishing and/or reviewing retention periods, the following shall be taken into account:
  - a) The objectives and requirements of the Company;
  - b) The type of personal data in question;
  - c) The purpose(s) for which the data in question is collected, held, and processed;
  - d) The Company's legal basis for collecting, holding, and processing that data (e.g. the Company being the subject of an audit by HMRC);
  - e) The category or categories of data subject to whom the data relates.

## 8. Roles and Responsibilities

- 8.1 The Company's Data Protection Officer is June Heather Dunnett.
- 8.2 The Data Protection Officer shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, the Company's other Data Protection-related policies (including, but not limited to, its Data Protection Policy), and with the GDPR and other applicable data protection legislation.
- 8.3 The Data Protection Officer shall be directly responsible for ensuring compliance with the above data retention periods.
- 8.4 Any questions regarding this Policy, the retention of personal data, or any other aspect of GDPR compliance should be referred to the Data Protection Officer.

## 9. Implementation of Policy

This Policy shall be deemed effective as of 25 May 2018. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

This Policy has been approved and authorised by:

**Name:** June Heather Dunnett, Director of the Company

**Date:** 25 May 2018