



Data Retention Policy 25th May 2018

1. Introduction

This Policy sets out the obligations of Red River Solutions Ltd, a company registered in the United Kingdom under number 5287691, whose registered office is at Red River Solutions Ltd, Unit 13, Natts Lane, Billingshurst, West Sussex, RH14 9EZ (“the Company”) regarding data protection and the rights of Clients, Employees, Business Contacts (“data subjects”) in respect of their personal data under 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 that are in the public interest, for scientific or historical research, or for statistical 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; or
- f) Where the personal data is processed for the provision of information society services to a child.

This Policy sets out the type(s) of personal data held by the Company, the periods(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. Please refer to section 6 and 7 below.

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 and by third-party data processors processing personal data on the Company's behalf.
- 3.2 Personal data, as held by the above is stored in the following ways and in the following locations:
 - a) The Company's servers.
 - b) Third-party cloud -based, password-protected systems.
 - c) Computers permanently located in the Company's premises.
 - d) Laptop computers and other mobile devices provided by the Company to its employees;
 - e) Computers and mobile devices owned by employees, agents, and sub-contractors used in accordance with the Company's Access Control Policy.
 - f) Physical records stored securely in the company's registered office.

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 (or, if no fixed retention period can be determined, the criteria by which the retention of the data will be determined).
- 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), 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 secure, see section 19 and 20 of our Data Security Policy.
- 5.2 The following organisational measures are in place within the Company to protect the security of personal data. Please refer to Part 24 of the Company's Data Protection Policy for further details.

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 held in electronic form shall be deleted from the companies servers, desktop computers, mobile devices and all backup media. Data held in paper form shall be securely shredded and disposed of by our approved contractors.

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) The category or categories of data subject to whom the data relates;
- 7.4 If a precise retention period cannot be fixed for a particular type of data, criteria shall be established by which the retention of the data will be determined, thereby ensuring that the data in question, and the retention of that data, can be regularly reviewed against those criteria.
- 7.5 Notwithstanding the following defined retention periods, certain personal data may be deleted or otherwise disposed of prior to the expiry of its defined retention period where a decision is made within the Company to do so (whether in response to a request by a data subject or otherwise).

7.6 In limited circumstances, it may also be necessary to retain personal data for longer periods where such retention is for archiving purposes that are in the public interest, for scientific or historical research purposes, or for statistical purposes. All such retention will be subject to the implementation of appropriate technical and organisational measures to protect the rights and freedoms of data subjects, as required by the GDPR.

Data Ref	Type of Data	Purpose of Data	Review Period	Retention Period or Criteria
Business Contacts	Work-based and sometimes personal contact details where provided of clients, suppliers and third parties	Business correspondence	Annually	5 years
Employee	Employee Personal Details	Salary and pension payments	Annually	5 years
Clients	Mailing Lists	Delivery of Consent based Direct Mail	Annually	30 days from mailing date unless specified by the client

8. Roles and Responsibilities

- 8.1 The Company's Data Protection Officer is Laura Ashton.
- 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 or The Information Security Manager shall be directly responsible for ensuring compliance with the above data retention periods throughout the Company.
- 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 or The Information Security Manager.

9. Implementation of Policy

This Policy shall be deemed effective as of 25th 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: John Baulch
Position: Managing Director
Date: 25th May 2018
Due for Review by: 25th May 2019
Signature:

