

Ramarketing & PR Limited
Data Retention Policy
November 2019

1. Introduction

This Policy sets out the obligations of Ramarketing & PR Limited, a company registered in United Kingdom under number 7672129, whose registered office (since October 2nd 2018) is at Ramarketing & PR Ltd. Sunco House, 5 Carlial Square, Newcastle upon Tyne, NE1 6UF ("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").

Ramarketing is registered with the Information Commissioner's Office. (ICO) In registering, Ramarketing has contractually committed to delivering its services in compliance with the Data Protection Act and the GDPR.

The ICO Registration number is: ZA333533. Date Registered: 27 March 2018. Date of Expiry: 26 March 2020.

This Data Retention Policy explains our requirements to retain data and to dispose of data and provides guidance on appropriate data handling and disposal in a GDPR compliant manner.

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:

- Where the personal data is no longer required for the purpose for which it was originally collected or processed (see above);
- When the data subject withdraws their consent;

- When the data subject objects to the processing of their personal data and the Company has no over-riding legitimate interest;
- When the personal data is processed unlawfully (i.e. in breach of the GDPR);
- When the personal data has to be erased to comply with a legal obligation; or
- 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 data processing on behalf of its clients for marketing purposes (i.e. research, e-mail marketing, direct mail) and its own data controller and processor for staff, clients, suppliers and business development & marketing purposes, 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.

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 Ramarketing & PR Ltd. For HR, client and supplier contacts, PR, marketing and business development purposes and by third-party data processors processing personal data on the Company's behalf (i.e. print suppliers).

3.2 Personal data, as held by Ramarketing & PR Ltd is stored in the following ways and in the following locations:

a) The Company's document storage systems - G Suite from Google including Gmail, Docs, Drive and Calendar. Full details available here https://gsuite.google.co.uk/intl/en_uk/

b) Third-party servers, operated by Whittle Print (preferred print suppliers) and located in 36 Hutton Cl, Washington NE38 0AH

c) All employees uses laptops and they are mobile workers. All company laptops are encrypted with 256 bit encryption and have anti-virus softwares. Subcontractors uses own laptops and adhere to Ramarketing's IT policy.

d) Laptop computers and other mobile devices provided by the Company to its employees;

e) Harvest for time tracking, invoicing, and reporting - <https://www.getharvest.com/>

f) Zoho CRM for customer relationship management - <https://www.zoho.eu/crm/>

g) Basecamp for task & project management - <https://basecamp.com/>

h) Asana for task & project management - <https://asana.com/>

4. Data Subject Rights and Data Integrity

Data Subjects are any living identifiable individuals whose information we collect. As a Data Subject, you have the following rights under the GDPR:

Right of Access: This right allows data subjects to access the personal information gathered by Ramarketing. Data subjects have the right to find out how their personal information is shared, stored, secured and processed on request.

Right to Correction: This right allows data subjects to request that any of their personal information at Ramarketing is corrected.

Right to Erasure (Right to be Forgotten): This right allows data subjects to request, subject to certain applicable legal limitations, that their personal information be erased from Ramarketing's possession.

Right to Complain: This right allows data subjects to make a complaint to the relevant supervisory authority about Ramarketing's handling of their personal information.

Right to Restrict Processing: This right allows data subjects to restrict how and why their personal information will be used and processed by Ramarketing.

Right to Object: This right allows data subjects to object to how or why their personal information is processed by Ramarketing.

Right to Portability: This right allows data subjects to receive the personal information Ramarketing has stored about them and it also allows data subjects to have that data transferred to a third party.

Right to not be subject to Automated Decision-Making: This right allows data subjects to prevent any decision that has a legal or similarly significant effect on the data subject being made solely on the basis of an automated decision. This right is subject to certain limitations under applicable laws within the European Union. It is also limited if the automated decision is necessary for the performance of a contract between Ramarketing and the data subject, or if the data subject provides explicit consent to automated decision-making.

All of these rights can be exercised by contacting Ramarketing directly. If you have any questions about these rights or wish to exercise them, please contact us at:

dataprotection@ramarketingpr.com

4.1 All personal data held by the Company is held in accordance with the requirements of the GDPR and data subjects' rights thereunder

4.2 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).

4.3 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, the right to data portability, and further rights relating to automated decision-making and profiling. The Company uses G suite and therefore adheres to its data retention, deletion and restoration policy. Specifically the Company can;

4.3.1 Restore data that was permanently deleted within the past 25 days.

4.3.2 Select a date range to restore data that was deleted within that range.

4.3.3 Check a user's Gmail inbox or Drive folder to confirm the data is restored.

4.3.4 Use Vault to restore Gmail messages. To find out more about data retention for Google Vault and G Suite see here:

https://support.google.com/vault/answer/2990828?hl=en&ref_topic=3209998

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.

5.1.1 All emails containing personal data or otherwise are encrypted;

5.1.2 All emails containing personal data must be marked "confidential";

5.1.3 Personal data may only be transmitted over secure networks;

5.1.4 Personal data may not be transmitted over a wireless network if there is a reasonable wired alternative;

5.1.5 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;

5.1.6 Where personal data is to be transferred in hardcopy form (i.e. staff details), it should be passed directly to the recipient sealed and marked confidential or sent using the companies preferred delivery service FEDEX;

5.1.7 No employee personal data may be shared informally and if access is required to any personal data, such access should be formally requested from the Company Secretary

5.1.8 No marketing personal data may be shared informally and if access is required to any personal data, such access should be formally requested from the designated Account Lead

5.1.9 All hardcopies of personal data, along with any electronic copies stored on physical media will be stored securely in lockable units accessed only by the Office Manager, Company Secretary, General Manager and Directors.

5.1.10 No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Company or not, without authorisation from designated Account Lead and/or Company Secretary or without the explicit consent of the data subject.

5.1.11 Personal data must be handled with care at all times and will not be left unattended or on view;

5.1.12 Computers used to view personal data will always be locked before being left unattended;

5.1.13 No personal data should be stored on any mobile device, whether such device belongs to the Company or otherwise without the formal approval of Senior Management Team and then strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary;

5.1.14 No personal data should be transferred to any device personally belonging to an employee unless via the G suite app and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Company where the party in question has agreed to comply fully with the Company's Data Protection Policy and the GDPR;

5.1.15 All personal data stored electronically should be backed up. The company aims to keep all electronic data backed up and is exploring new ways to ensure all personal data stored electronically is backed up.

5.1.16 All electronic copies of personal data should be stored securely using passwords and encryption;

5.1.17 All passwords used to protect personal data should be changed regularly and should must be secure;

5.1.18 Under no circumstances should any passwords be written down or shared. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords;

5.1.19 All software should be kept up-to-date. Security related updates should be installed as soon as reasonably possible after becoming available;

5.1.20 No software may be installed on any Company-owned computer or device without approval; and

5.1.21 Where personal data held by the Company is used for marketing purposes, it shall be the responsibility of the account lead to ensure that the appropriate consent is obtained and that no data subjects have opted out, whether directly or via a third-party service.

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

5.2.1 All employees and other parties working on behalf of the Company shall be made fully aware of both their individual responsibilities and the Company's responsibilities under the GDPR by attending the Company 'GDPR Awareness training sessions' and additional training on client data handling, security and all policy detail to ensure continuous compliance. All current employees have been trained pre-25 May 2018. The Company has also taken measures to ensure that all other parties have sufficient accreditation or compliance procedures to handle personal data.

5.2.2 Only employees and other 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. In the case of processing client data this will be restricted to account specific employees and contractors only;

5.2.2.1 All employees and other parties working on behalf of the Company handling personal data will be appropriately trained to do so;

5.2.2.2 All employees and other parties working on behalf of the Company handling personal data will be appropriately supervised;

5.2.2.3 All employees and other parties working on behalf of the Company handling personal data should exercise care and caution when discussing any work relating to personal data at all times;

5.2.2.4 Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed annually alongside our existing policies;

5.2.2.5 The performance of those employees and other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed;

5.2.2.6 All employees and other 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;

5.2.2.7 All agents, contractors, or other parties working on behalf of the Company handling personal data must ensure that any and all relevant

employees are held to the same conditions as those relevant employees of the Company arising out of the GDPR and the Company's Data Protection Policy;

5.2.2.8 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 using <https://sourceforge.net/projects/eraser/> or G suite deletion processes which permanently erases data after 25 days.

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) The category or categories of data subject to whom the data relates;
- f) If an individual has a legitimate interest* for retention.

*When determining a lawful basis for data retention, Ramarketing will consider the purpose of the legitimate interest that the data subject has, whether it is necessary to retain the data for longer and we will additionally consider how this may affect other data subject's rights.

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.

NB this is not an exhaustive list and will be updated continually.

Data ref	Type of data	Purpose of data	Retention period	Comments
ZoHo CRM	Customer contacts	Marketing communications		Reviewed in alignment with the client contracts
ZoHo CRM	Lead contacts	Marketing communications and legitimate interest	3 months	Erased if no contact has been received
Harvest and Zero	Client contacts	For billing and project tracking	180 days	12 months post contract end date (this may extend to 5 years with company only detail for data tracking purposes NOT personally identifiable details)
Mailing lists	Client contacts	For marketing communications	12 months	12 months post contract end date
People HR software and Google Drive	Staff	For employee files	Permanently unless employment has ceased	6 years termination of contract. Please note it can take up to 15 days for files to be removed from the drive after the retention period has expired.

Google Drive	Job applicants	For recruitment	6 months	Store for 6 months after post filled. Please note it can take up to 15 days for files to be removed from the drive after the retention period has expired.
Basecamp	Customer contact details	To provide clients with access to basecamp and receive notifications		After account closure, the data remains in Evernote's possession for 30 days. After that, it is deleted.

8. Litigation

In the event of actual or contemplated litigation or once an official or regulatory investigation has begun, the operation of this Data Retention Policy will be suspended for any data or metadata that is relevant to the dispute or investigation to ensure its preservation.

9. Transferring Personal Information outside of the European Economic Area (EEA)

Ramarketing will not transfer a data subject's personal information outside the EEA unless such a transfer is compliant with the GDPR.

Ramarketing will only transfer personal information to another jurisdiction outside the EEA if the jurisdiction has been approved by the European Commission to meet the GDPR's data protection standards. Such transfers are subject to appropriate safeguards, which may include standard data protection clauses, binding corporate rules or any derogation in the GDPR. (Including explicit consent)

Where Ramarketing transfers data to the United States, we will transfer data in accordance with the requirements set by the Privacy Shield which applies a similar level of protection to personal data as the GDPR.

10. Roles and responsibilities

10.1 The Company's Data Protection responsibilities lie with the relevant account lead or Senior Manager for Data processing of client details. Employee information is the responsibility of the Company Secretary.

10.2 The Board (Directors) shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this GDPR Policy.

10.3 Any questions regarding this Policy, the retention of personal data, or any other aspect of GDPR compliance should be referred to

dataprotection@ramarketingpr.com and will be dealt with by the relevant personnel.

11. Implementation of policy

This Policy shall be deemed effective as of 23 May 2018. This policy was updated on 11 November 2019. 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: Raman Sehgal

Position: Founder and Managing Director

Date: 23 May 2018

Policy reviewed: 11 November 2019

Due for Review by: 11 November 2020

Signature:

A handwritten signature in blue ink, appearing to read 'Raman Sehgal', is positioned below the 'Signature:' label.