CMS Direct Mail Ltd
Data Retention Policy April 2018

1.0 Definitions

"The Company":	CMS Direct Mail Limited
"The Client":	The person for whom The Company has agreed to provide a specified service
"Specified Service":	The service to be provided by The Company for The Client
"Backup":	Any data copied to a second location, solely for the purpose of safe keeping of that data.
"Encryption":	The process of encoding data with an algorithm so that it is unintelligible and secure without the key. Used to protect data during transmission or while stored.
"Encryption Key":	An alphanumeric series of characters that enables data to be encrypted and decrypted.

2.0 Purpose
The purpose of this policy is to specify The Company's guidelines for retaining data supplied by The Client.

3.0 Scope
The scope of this policy covers all data supplied by The Client to The Company.

4.0 Policy
Data will only be retained until reasonable future need no longer exists. All data supplied by The Client will automatically be deleted from systems, servers and backups no later than 8 weeks after the Specified Service has been completed.

4.1 Retention of Encrypted Data
If any information retained under this policy is stored in an encrypted format, encryption keys will be stored in The Company safe and/or within a password protected document. Encryption keys must be retained as long as the data that the keys decrypt is retained.

4.2 Data Destruction
When the retention timeframe (8 weeks after the Specified Service has been completed) expires, data covered by this policy will be automatically deleted.