DATA & RECORD RETENTION POLICY

INTRODUCTION

We are obliged as an organisation, both by law and corporate governance, to protect the integrity and confidentiality of personal data held by us with regard to our clients and employees. Individual employees also have that obligation. However you decide to compile your database, it is vital to make sure that both parties stay legally compliant.

Under no circumstances will your data ever be made available, sold to third parties or otherwise marketed.

Integrity lies at the heart of Bulk SMS Limited. The trust that we inspire in our customers and stake-holders is the key to our success as an organization and as individuals. As leaders in our industry, we hold ourselves to the highest standard of professional behavior. The Bulk SMS Limited Code of Integrity defines the main principles of professional integrity for the Bulk SMS Limited Group and is an expression of the values that are shared throughout our organization, our businesses and our affiliates.

This Data Protection Policy has been written to assure Bulk SMS Limited employees know their duties under the General Data Protection Regulation (GDPR) and Record Retention procedures. This policy also states the standards expected by Bulk SMS Limited employees in relation to processing of personal data and safeguarding individuals 'rights and freedoms'. Bulk SMS Limited is registered and by all means committed to following GDPR.
It is very important to us that we take a serious view of our responsibilities and make sure each appropriate individual complies with Data Protection principles. If you knowingly reveal any personal data contrary to this policy, you may be held liable to criminal sanctions. Also, any breach of this policy may result to a disciplinary action.

Article 5 of GDPR requires that personal data shall be:

"**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."

PERSONAL DATA

"Data" means information recorded in a form in which it can be processed by equipment operating automatically in response given for that purpose and also includes computer-generated material. "Personal Data" means data that consists of information that is related to a living individual who can be identified from that given information including any expression of opinion about the individual. This means any data recorded on our computers relating to a living individual.

Personal data must:

- be held and processed fairly and lawfully;
- be obtained only for the purposes of which it is registered
- by used only for the purposes registered and only be revealed to those described in the register entry
- be relevant, adequate and not excessive in relation to those purposes
- be correct and when necessary, kept up to date
- only be kept for the amount of time that is necessary

An individual is entitled to:

- be informed when the personal data that is entered is held
- access any given data
- have such data corrected, when needed
- the right to erasure
- the right to restrict processing
- the right to data portability
- the right to object

To comply with the core principles of GDPR and ePrivacy, records containing personal data must be:

- Stored appropriately in regards to the sensitivity and confidentiality of the data recorded
- Easily traced and retrievable
- Obtained for only as long as necessary
- Removed within prescribed timescales when requested
- Disposed of appropriately and properly to ensure that copyrights are not breached and to prevent the data falling into the hands of an unauthorised individual

Appropriate security procedures must be taken place against unauthorised access to or alteration, destruction or disclosure of personal data or accidental loss or destruction of personal data.

CLIENT DATA

This section specifically states the responsibilities of data held which is owned by our clients and includes the recording, processing and security of personal and sensitive information relating to them and the people who work for them.

Whilst it is completely our responsibility to ensure that the personal data held regarding our client is up to date, accurate and taken for lawful purposes, it is your duty to ensure that the information taken from your clients is correct and accurately entered on to our database.
It is also our responsibility to make sure that the database and portal is backed up on a regular basis and to ensure there is no loss of personal data. If you come across any errors or have concerns regarding personal data you must report these straight away to your account manager or support team.

Appropriate security procedures must be taken against:

- unauthorised personnel having access to or alteration, or destruction of personal data.
- accidental loss or destruction of personal data.

Data that is related to a client will never be disclosed to third parties unless the client has given consent. Under no circumstances are third parties ever given access to client data, unless under legal, legislative or regulatory instruction.

BULK SMS LIMITED EMPLOYEES DUTIES

Bulk SMS Limited employees are expected to:

- Be aware of and abide by the Data Protection Principles
- Read and understand the Bulk SMS Limited Data Protection Policy and Service Agreement.
- Understand how to work to the set standard that is expected at any stage of the data life-cycle
- Understand how to work to the set standard that is expected in relation to safeguarding data subjects rights, e.g. the right to inspect any personal data under GDPR and ePrivacy.
- Understand what is meant by 'sensitive personal data' and how to handle such data.

RETENTION

Data and records will only be kept for the minimum time. This is a principle found in GDPR, which states that data controllers must ensure that 'the period for which the personal data are stored is limited to a strict minimum".

No data file or record should be obtained for the maximum period unless a reason for longer retention can be put into place.

After the retention period has expired, some records may be kept permanently for historical purposes. Reasons they may be kept is that they may preserve evidence of the origin, development, or other reasons for longer retention which include the following:

- Statute requires retention for a longer period of time
- The record contains information that is relevant to legal action that has been or is taking place
- Whenever there is a possibility of litigation, the records and information that is involved should not be amended or disposed of until the threat has been removed
- The record should be archived for research or historical use, for example if the record has information that relates to an important policy development
- The records are kept for the purpose of retrospective comparison.
- The records relate are related to individuals or providers of certain services who may be judged as unsatisfactory.
- The said individuals may include Bulk SMS Limited employees who have been the subject of serious disciplinary action.

GUIDELINES FOR DATA PROTECTION

Personal data must be processed according to the six data protection principles:

- Processed lawfully, fairly and transparently.
- Collected only for specific legitimate purposes.
- Adequate, relevant and limited to what is necessary.
- Must be accurate and kept up to date.
- Stored only as long as is necessary.
- Ensure appropriate security, integrity and confidentiality.

Personal Data will only be held for the amount of time that it is needed, in this case for 24 months since last used by the customer unless otherwise instructed by the customer. When the data is at a point where it is necessary for said data to be destroyed, appropriate measures will take place to ensure the data cannot be used again by third parties. Any file or record that contains personal data will be considered as confidential.

DESTRUCTION AND DISPOSAL

To make sure that Bulk SMS Limited follow GDPR and all information in any format, destroyed from any Bulk SMS Limited location must not expose confidentiality of our employees, clients and customers.

- All office white or coloured paper will be disposed of using accredited confidential waste disposal suppliers

As company policy, Bulk SMS Limited does not utilise electronic media such as memory sticks, flash drives, tape, cassette/cartridge, hard drives, CD-Rom, DVD, ZIP drive.

Customer Data

- Any account that has not been accessed for 24 months will be deleted including but not limited to:
  - Account specific information
  - Any list containing a number, to include but not limited to contact lists, whitelists and blacklists
  - SMS sent and received
  - IP Addresses stored in logs relating to the customers account
  - This will be completed within 10 business days after the 24 month period
- At the request of a customer to delete their data permanently the following information will be deleted including but not limited to:
  - Account specific information
  - Any list containing a number, to include but not limited to contact lists, whitelists and blacklists
  - SMS sent and received
  - IP Addresses stored in logs relating to the customers account
  - This will be completed within 10 business days from receiving the request
- Right To Erasure “RTE” / (Right to be forgotten) for a specific contact
  - Should a customer, of Bulk SMS Ltd, receive a right to erasure (right to be forgotten) request, then Bulk SMS Ltd will provide various methods to remove any data. These methods will be made available to the customer via the portal and the API. Once a request has been received, the data will be deleted from the platform and all backups within 10 business days.
  - RTE’s will not be accepted via phone or email unless there is a support issue arising to a customer not being able to lodge the RTE request via normal methods.
- Specific requests by customers to not store data older than ‘X’
  - Should a customer with Bulk SMS not wish to store data older than ‘X’ weeks / months / years, a support request should be submitted to Bulk SMS Ltd to request this.
- Support Requests when uploading contact information
  - Customers requiring support when uploading data into the Bulk SMS Ltd Portal will need to

submit the file to support via the portal.

- This will provide customers with a secure method of transferring files to Bulk SMS Ltd
- Once the support request has been completed, any files uploaded by the customer will be deleted from the Bulk SMS Platform within 24 hours of completion. Any file uploaded for support will not be backed up by our automated solution and therefore any file stored once deleted can not be restored

- Any file containing customer data, e.g. a contact list, received via email or electronic file share will be instantly deleted by Bulk SMS Ltd. The email address that sent the file will be notified within 8 business hours that the file was deleted and not processed

- Files uploaded by a customer for importing into the Bulk SMS platform
  - These are securely stored on whilst the file is imported into the platform
  - Files will not be stored on the platform for longer than 24 hours after the file was uploaded
  - Files uploaded will not be backed up by the automated backup solution and therefore any file stored once deleted can not be restored