GDPR COMPLIANCE WHITE PAPER

8 March 2018

1. Introduction

The European Union's General Data Protection Regulations ("the GDPR") impose a broad range of obligations on "data controllers" and on "data processors" who process the personal data of "data subjects" (meaning identifiable natural persons in terms of Article 4 of the GDPR).

In our business we act both as "data controllers" (e.g. where we manage client data) and as "data processors" (e.g. where we transmit messages on behalf of our clients to a range of message recipients, many of whom may be identifiable natural persons or "data subjects" and whose personal data may include names, telephone numbers and email addresses).

This GDPR white paper details the obligations imposed on us by the GDPR and the steps we have taken to ensure full compliance.

We take personal data protection seriously and have given careful consideration to all of the obligations imposed on both data controllers and data processors in terms of the GDPR and have put in place appropriate measures to ensure that we comply not only with the letter but the spirit of the GDPR too for the benefit of our clients and the persons to whom they may deliver messages using our services.

2. Lawfulness of Data Processing

In terms of the GDPR, we may only process personal data:

- lawfully, fairly and in a manner transparent to data subjects;
- for a specified, explicit and legitimate purpose;
- that is accurate, adequate, relevant and limited to what is necessary in relation to the purpose for which we are processing the data;
- that is accurate and up to date;
- that is kept in a form permitting identification of data subjects for no longer than necessary; and
- that is processed in a manner ensuring appropriate security using appropriate technical and organisational measures.[1]

Our processing of personal data is only lawful if:

- consent has been given by the data subject to the processing of their personal data for a specific purpose;
- it is necessary for the performance of a contract to which the data subject is a party;
- it is necessary in order for us to comply with a legal obligation to which we are subject; or
- it is necessary to process the data or where the legitimate purpose for which the data is processed are not overridden by the privacy interests or other rights of the data subject.[2]

We ensure that we meet our obligations to only process data in a lawful and fair manner by categorizing and inventorising the personal data that we process or hold and by regularly assessing our data privacy practices including the current technologies we use to process personal information and to deliver our services to our clients.

[1] Article 5 of GDPR (all subsequent notes are shortened to the article reference).
[2] Article 6.

3. Technical and Organisational Measures

In terms of the GDPR we are required to **implement appropriate technical and organisational measures** to ensure the security and protection of personal data including through techniques such as data anonymisation and other "privacy by design" techniques[3] and to integrate necessary safeguards into our data processing activities.[4]

We ensure that we meet these obligations by taking a range of technical and organisational measures including the pseudonymisation and encryption of personal data, by regularly testing, assessing and evaluating the effectiveness of our measures including the resilience and availability of our information systems and our ability to quickly restore access to personal data in the event of a physical or technical incident.

4. Fair and Transparent Communications

The GDPR requires us to communicate fairly and transparently with our clients and data subjects regarding the collection and processing of personal information.[5]

We do this by ensuring that where personal data is collected, we provide information that is concise, easily accessible and using clear and plain language.

Where the GDPR obliges us to furnish a person on request with information regarding whether or not personal data concerning him or her is being processed[6] or how such data may be disclosed, we provide that information and a copy of all such data undergoing processing without delay, free of charge for the first such request, and we notify the requester that he or she may lodge a complaint with a supervisory authority where not satisfied with our response.
Where we collect personal data directly from a data subject as a data controller, the GDPR requires us to provide the data subject with the following information:

- our identity and contact information for our business and our data protection officer;
- the purposes and legal basis of the processing for which the personal data are intended, including, where our processing is based not on the data subject's consent but on our "legitimate interests", and what those legitimate interests are;
- the intended recipients or categories of recipients of the personal data.[7]

We have ensured our compliance with these obligations by reviewing our disclosure and notification processes, including within our business terms and conditions and privacy policies, by reviewing the methods and mechanisms by which we obtain and record consent of data subjects; by conducting data protection impact assessments; by creating a data privacy governance structure involving senior management to establish the ongoing tasks, responsibilities and reporting lines of persons involves in ensuring continuance compliance with the GDPR including but not limited to through the establishment of a Data Protection Officer; and by engaging our staff in training on our personal data protection standards, policies and procedures.

Where our processing of personal data is based on consent, then the GDPR requires us to be able to demonstrate that the data subject has consented to the processing of their personal information, to permit the data subject the right to withdraw their consent and to inform the data subject of their right to do so.[8]

[3] Article 18.
[4] Articles 24 and 25.
[5] Article 12.
[6] Article 15.
[7] Article 13.
[8] Article 7.

5. Rectification and Erasure of Data

We are also obliged in terms of the GDPR to rectify any incorrect personal data upon the request of the data subject[9] and to erase the personal data of a data subject without undue delay where the personal data is no longer necessary in relation to the purposes for which it was collected or processed; or where the data subject withdraws his or her consent or legitimately objects to the processing and there are no overriding legitimate grounds or other lawful grounds for processing.[10]

A data subject also has the right to request restricted processing of his or her personal data where we act as a data controller in relation to his or her personal data and where:

- the accuracy of the personal data is contested and while we verify the accuracy of the data;
- the data subject has objected to processing pursuant to our "legitimate interests", pending the verification of whether our legitimate grounds override the objection of the data subject; and
- the personal data is no longer needed by our business but is required for the establishment, exercise or defence of legal claims.[11]

We will comply with any rectification, restriction or erasure request where we are obliged to do so and we will also communicate any rectification or erasure of personal data, or restriction of processing carried out to each recipient to whom we have disclosed the personal data, unless it is impossible for us to do so or involves disproportionate effort.[12]

6. Objections to Processing

We are also obliged in terms of the GDPR to cease processing of personal data concerning a data subject where the data subject has objected, unless compelling legitimate grounds can be shown which overrides the rights and interests of the data subject.

Where personal data is processed for direct marketing purposes, the data subject has the right to object at any time and the personal data will no longer be processed for those purposes. We ensure that we comply with this obligation by, amongst other things, offering an automated opt-out mechanism as part of all marketing communications, including our promotional newsletters and other marketing communications.[13]

7. Accessibility and Interoperability of Personal Data

The GDPR requires us to make personal data regarding a data subject available to him or her upon request in a structured, commonly used and machine-readable format to enable that data to be transmitted to another controller without hindrance.[14]

We comply with this obligation by ensuring that all of our information systems that host or process personal data are capable of exporting that data to common machine-readable formats, such as CSV files or SQL 'dumps' and by enabling our clients to export their address books stored within our information systems.

[9] Article 16.
[10] Article 17.
[11] Article 18.
[12] Article 19.
[13] Article 21.
[14] Article 20.

8. Third Party Processing

Where we act as data controller and engage a third party to performing data processing on our behalf, we are obliged in terms of the GDPR to use only processors providing sufficient guarantees to implement appropriate technical and organisational measures so as to meet the requirements of GDPR, and, where we act as data processors, we are not permitted to engage another processor without the prior written authorisation of the controller.

We ensure in all of our data processing agreements that the agreements clearly record the subject-matter to be processed, the nature, purpose and duration of processing and all the contractual stipulations itemised in Article 28(3)(a) to (g) of the GDPR.[15]

9. International Data Processing

Where a part of our business is based outside of the European Union but is processing the personal data of subjects in the Union, we are required to designate a representative within the Union who is mandated to deal with the relevant supervisory authorities and data subjects on all issues related to personal data processing.[16]

Our business has appointed a representative of our United Kingdom office as our European Data Protection Representative. Subject to the anticipated departure of the United Kingdom from the European Union our business will appoint a representative of one of our other European regional offices as our EU Data Protection Representative.

The GDPR requires us not to transfer any personal data to a third country for processing unless that country is also a member of the European Union and bound by the GDPR or unless the third country has been designated by the EU as a country of trust or safe harbour. We may only transfer data for processing to an organisation that is not part of the EU or a safe harbour where we have ensured through contractual and other mechanisms that the receiving organisation shall ensure a level of protection for the personal data that is adequate and appropriate in terms of the standards of the GDPR.[17]

We comply with this obligation by identifying all circumstances in which personal data may be transferred to recipients located outside of the European Union and by entering into appropriate agreements with receiving parties ensuring that, for each such transfer, the receiving party has in place a data transfer mechanism that complies with the requirements of the GDPR.

10. Responding to Breaches

In the event that we ever experience a personal data breach, our **Incident Response Policy** ensures that we shall notify the relevant supervisory authority and keep a record of the breach without undue delay and, if possible, by not later than 72 hours after having become aware of the breach.[18] If the breach is likely to result in high risk to the rights of natural persons, then we will communicate the breach to the data subject without undue delay to comply with our obligations in terms of Article 34 of the GDPR.

[15] Article 28.
[16] Article 27.
[17] Article 44 to 50.
[18] Article 33.

11. Additional Obligations

Depending on the nature and size of a data controller's or processor's business, additional obligations may be imposed by the GDPR including the requirement to keep a record of the data processing activities of the business such as the purposes of processing, the categories of personal data held and the nature of the data transfers engaged in by the business.[19]

Although our own organisation is not legally obliged under the GDPR to deliver these types of records on request, our **Promotion of Access to Information Policy** records the nature and types of records that we keep and the processes by which access to these records may be obtained. Our Promotion of Access to Information Policy manual may be accessed via our website at BulkSMS.com.

12. National Data Protection Authorities

National Data Protection Authorities or "DPA's" are independent public authorities that supervise and investigate the application of the GDPR in EU Member States. There is one in each EU Member State.

Generally speaking, your main contact point for issues relating to data protection is the DPA in the EU Member State where your organisation is based. However, if your organisation processes data in different EU Member States or is part of a group of companies established in different EU Member States, that main contact point may be a DPA in another EU Member State.

A full list of EU DPA's is available here.

13. Data Protection Officer Contact Details

Data Protection Officer

Dr Pieter Streicher, Managing Director: BulkSMS.com
1st Floor, Mazars House
Rialto Road, Grand Moorings Precinct
Century City, Cape Town
7441
South Africa
Tel: +27 (0) 21 552 6321
Fax: +27 (0) 21 552 2848
Email: privacy@BulkSMS.com

European Data Protection Representative

Dan Perrin, Product and Business Development UK: BulkSMS.com
Basepoint Business and Innovation Centre
Metcalf Way
Crawley, West Sussex
RH11 7XX
United Kingdom
Tel: 0345 40 30 767
Fax: 0845 01 777 65
Email: dan@BulkSMS.com

[19] Article 30.