What is Messaging Compliance?

Understanding who you are Getting Consent from, for what & how?

Businesses are required to obtain specific consent before messaging their prospects and customers. Each regulation such as Telephone Consumer Protection Act (TCPA), General Data Protection Rights (GDPR), Canada's Anti-Spam Legislation (CASL), or California Consumer Privacy Act (CCPA), California or the new California law, makes it mandatory for each business to obtain specific consent. SMS Magic has created an extensive framework which serves as a guideline for you to define:

- Who are you messaging?
- What you are messaging and obtain specific consent for that content?
- How you are obtaining Consent?

There are several considerations in choosing your consent options. We advise you to consult your attorneys before deciding on the messaging consent.

Three Keys to Compliance – Write, Map, and Configure

Write	Map	Configure
1. Current consent methods	1. Current consent methods to SMS use cases	1. Consent database
2. SMS use cases	2. Decide on double opt-in or confirmation via SMS	2. Consent for source and specific content
		3. Double opt-in’s
		4. Keywords and confirmation messages

Choosing a Consent Database

The applicable laws like TCPA and GDPR make it mandatory to obtain consent and keep records in a readily available audit database which can be used as evidence in case of a dispute. This database of Consent records needs to be maintained for 4 years (as per GDPR) from the date of its creation.

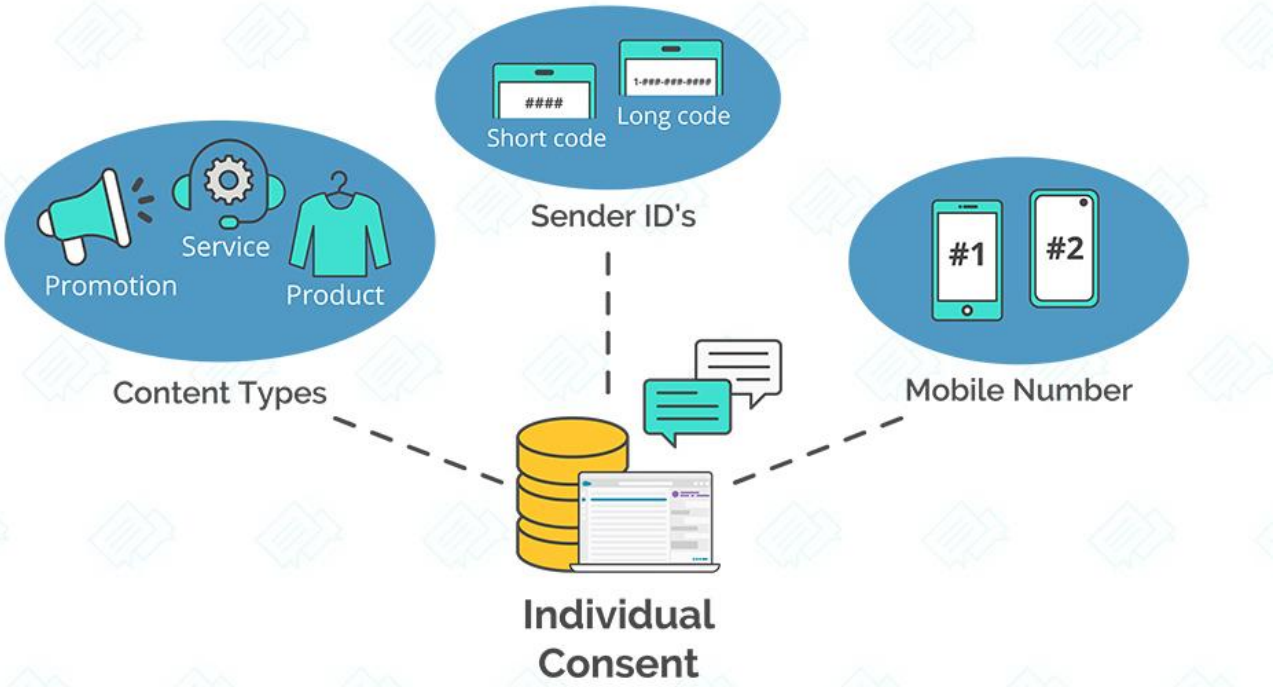
With SMS Magic you can choose how you obtain and maintain or record your consent. You can choose to get a blanket consent for sending any legally possible Content or get a specific Consent. For example, you can get blanket consent for sending any type of messages, service, transactional, or promotional; Or you can get specific consent for sending transactional messages only.

This specific consent is recorded via Sender ID and Content

Type. You can choose any of the following methods:

- **Mobile Number Only** – You Opt-in to have a blanket yes or no consent for any recipient
- **Mobile Number and Sender ID** – You record consent for specific Sender ID's. You always have the option to choose "All", while creating your consent records.
- **Mobile, Sender ID, and Content Type** – You choose to do specific consent based on Content Type.

We recommend using the Mobile number and Content Type to be specific. If you are obtaining blanket consent, then choose "All".



The compliance feature helps you create a consent database based on all these parameters. You can also enable users to create a consent record manually. However, users need to be provided with relevant permissions to create and update the consent database.

You can define consent record parameters in the following four possible combinations:

Parameter	Description
Mobile Number	When you enable mobile number as a record parameter, all consent will be accepted only when responses are received through the default mobile number the customer provides. This is a mandatory parameter and will have to be included in every combination.
Mobile Number and Sender ID	When you enable this parameter, consent records will be registered when responses are received from the registered mobile number and by the defined sender ID of the customer.
Mobile Number, Content Type, and Sender ID	When you enable this parameter, consent records will be registered against responses received from the defined phone number of the customer, for a specified Content-Type sent to the customer, and by the Sender ID of the user.

The compliance feature helps you create a consent database based on all these parameters. You can also enable users to create a consent record manually. However, users need to be provided with relevant permissions to create and update the consent database. For more information about creating a consent database, see Create a Consent Database.

Configure Double Opt-in

Many times businesses obtain consent to send messages via Web forms, emails or offline methods like contracts. Many industry bodies and associations like the TCPA recommend confirming the Opt-in via handset by sending an explicit SMS asking to confirm or at least notify the recipient that they are subscribed to the text message service from your business.

The consent status of the recipients is set to pending until they use this keyword to confirm the request. On receiving the keyword from the prospect, you send a response confirming the consent. This completes the compliance process. For more information about configuring double opt-in, see Configure Double Opt-in.

Configure Consent for Source and Content Type

This denotes for what type of content in your messages you are obtaining consent. The content can be defined by the source of the message (available with Start) or the Content Type (available with Grow).

Most regulations look at obtaining consent for automated or bulk SMS so you have to be careful while sending Content from different sources. A manually typed message is treated differently than a bulk or an automated SMS.

There are two options for defining what you obtaining consent for:

Source Type – You can define if the source requires a prior consent or not. For example, you might not require consent for sending an Emergency message. Another scenario is that you might not be required to use SMS-Magic Compliance Center because you have built your own compliance center. So you can choose, “Consent Not required”.

Content Type – Content type opt-ins are useful in ensuring that you can continue sending messages to customers for a specific content-type. Therefore, in case the customer is applying for a blanket opt-out instruction, in the opt-out confirmation message they receive, you specify the content type opt-in they can send if they wish to continue receiving messages for that specific content type.

For more information about configuring consent, see Messaging Compliance.

Configure Keywords

To comply with industry standards, you must respond to keywords for HELP & STOP. Any user who opts-out using the STOP keyword must be added to an opt-out list (blacklist) and must not be sent any further messages until or unless they opt back in. You can configure mandatory keywords for the three keyword types provided. These are:

- Opt-out
- Opt-in
- Help

For each keyword type, some default keywords have already been pre-defined. You can also create new ones following industry-specific norms.

Create keywords using the following guidelines:

- Use Alphabets
- Do not add spaces
- Do not include special characters

When a customer uses the keywords defined under the Opt-out keyword type, they will be opted out or blocked from receiving messages for all campaigns and other activities. You cannot send any more messages to all such customers.

Similarly, when a customer uses the keywords defined under **Opt-in** keyword type, they choose to opt-in for receiving messages from any team within the organization.

You can define separate keywords to help customers opt-in for specific content type messages, for example, notification or promotions. These keywords will be considered for receiving consent for that specific content-type.

Content-Type opt-ins are useful in ensuring that you can continue sending messages to customers for a specific content-type. Therefore, in case the customer is applying for a blanket opt-out instruction, in the opt-out confirmation message they receive, you specify the content-type opt-in they can send if they wish to continue receiving messages for that specific content-type.

For more information about configuring keywords, see Configure Keywords.

Upload Existing Consent Database

We store the consent record in ***Converse 1.59*** differently as compared to the previous version of *SMS-Magic Converse*.
Prior to the 1.59 release, we used to store consent information like Opted-In or Opted-Out on the object record detail page. The disadvantage of this style of storing consent information is that if the same number exist for two lead records and one record has opted-in and another record has opted-out information. The system will block one message but will still send the message to another record.

To overcome the above problem, we maintain consent information in *Consent* object and not at the object record level. These consent records are referred to when a user attempts to send messages via bulk, automated or manually. So, for example, the *Bulk* source, the *Consent Required* is configured, the system will always check for an Opt-In entry in *Consent* object. For more information about content databases, see Upload Existing Consent Database.