GUIDE

SMS-Magic

Regulatory Compliance for SMS Text Messaging in North America and the European Union

Introduction

Text messaging falls under the same regulatory compliance laws as email and phone communications. These regulations vary greatly by country, and are becoming more stringent every year, thanks to the onslaught of spam and need for privacy in our digital world. Companies using business messaging must meet the regulatory requirements for the geographies and carriers in which they do business. Violating these standards can result in heavy fines and blocked communications.

The diversity of regulations across different countries creates additional complexity for business text messaging users and administrators. This guide offers key insights and best practices recommendations into the regulations and requirements in major geographies around the globe.

Since regulations change dynamically, we recommend that you work with a vendor who understands the regulatory requirements in your geographies, and who actively monitors changes and updates to protect you and your business from the potentially significant consequences of non-compliance.

This guide is organized by regulatory bodies and geographic regions to make it easier for you to find your local regulations.

Regulatory Compliance in the US

Telecommunications in the United States is governed by the Federal Communications Commission (FCC), the managing body for regulating communications by satellite, wire, radio, television, cable, and text marketing. There is also an organization called the Cellular Telecommunications Industry Association (CTIA), a trade association that represents all wireless communication in the US. The CTIA offers recommendations and guidance for communication over wireless devices, but is not a legally governing body.

Legal compliance for business text messaging in the US is defined, moderated and managed by the Telephone Consumer Protection Act (TCPA). Here's the full TCPA if you want to read the details.

Telephone Consumer Protection Act (TCPA)

The TCPA defines compliance guidelines for all telephone communications, including auto-dialed calls, unsolicited fax messages, telemarketing calls and pre-recorded calls. Since text messages are considered similar to transactions like phone calls, they are also included within TCPA's responsibilities. TCPA has also defined anti-telemarketing laws for text messages.

The TCPA guidelines focus heavily on controlling SPAM communications in phone, email and text messaging.

SPAM is defined as an unsolicited advertisement. It applies to any material promotion for the commercial availability or quality of any property, goods, or services which is sent to any person without the recipient's prior express invitation or permission, in writing or otherwise.

In other words, customer consent is one of the mandatory

prerequisites to avoid being blocked for spamming, e.g., sending out unsolicited messages.

According to the FCC guidelines, a company can't send text messages to an individual's mobile unless the text has been sent in case of an emergency or the individual has given prior consent to receive the text.

Customer Consent for Business Text Messages

Customer consent is a critical requirement for business text messaging. As a business owner, you need to maintain a record of written consent shared by your customers prior to sending out text messages. You also need to clearly disclose that the customer is agreeing to being contacted in the future via text message.

This written consent can be in the form of a physically signed agreement, a digitally signed agreement or an SMS opt-in. You may also use a website form to ensure that you capture and retain the appropriate consent.

Whatever the mode of receiving consent, it must be compliant with federal and state law guidelines. Some of the accepted methods include text message, email, voice recording, website form, or phone entry.

Ensure that you state your terms and conditions clearly for your customers. They should be aware of the following:

- By acknowledging or signing the agreement, the customer is authorizing the company to send a specific type of content via messages.
- Consent is not a condition to buy any goods, services or property.

Be sure you map customer consent to a specific type of message content. This ensures that even if customers opt out of one type of message campaign, you are still able to communicate with them through other message types.

TCPA requires that you store consent for at least four years.

Essential Information for Promotions to Obtain Consent (Opt-in)

Before sending out promotions to request customers or prospects share their phone numbers, there are things you need to keep in mind.

When you ask for a buyer's mobile number, you need to disclose:

- The name of the program, its content and message frequency.
- A URL displaying the complete terms and conditions including your privacy policy, help and opt-out information.

Exceptions

You can send messages to customers without prior written consent only in a few scenarios. These include:

- **When you respond to a customer query** - If a customer asks for information, you do not require consent to respond to that request with the relevant information via text messages. However, it is important to remember that you can only send a single message immediately after you receive this request. Your message should contain only the information requested, without any other marketing information.
- **To check number reassignment** - You can also send out a single text message to check if a number has been reassigned to another subscriber.

Requirements for Compliant Consent

After a customer opts-in by sending a text message, you need to respond with a confirmation text message. This response message should also be legally compliant.

TCPA guidelines say that confirmation messages must include the following information:

- Your company name.
- Fulfill the offer that compelled the opt-in. In other words, your message content should include the content offered when the customer chose to opt-in.
- The frequency of messages to expect.
- Disclose possible carrier costs and fees.
- Give a keyword option to ask for help and opt-out of future texts.

You need also to be aware of the following regulations regarding TCPA compliant texting:

- Your campaign is considered inactive if you fail to send a message to a respondent within 18 months of their having opted-in for your program(s).
- Contests, sweepstakes, and lotteries are governed by state laws, which varies from one state to the other.
- If you are running contests, you must assign a registered short code for these types of campaigns. Carriers do not support running contests and will block these campaigns if they are not registered.

TCPA Guidelines for Text Spamming

TCPA guidelines for text messaging include a potential fine of $500 for every marketing text that violates TCPA regulations.

The TCPA guidelines specifically note the following:

"PRIVATE RIGHT OF ACTION—A person or entity may, if otherwise permitted by the laws or rules of court of a State, bring in an appropriate court of that State—

> **(A)** an action based on a violation of this subsection or the regulations prescribed under this subsection to enjoin such violation,
>
> **(B)** an action to recover for actual monetary loss from such a violation, or to receive $500 in damages for each such violation, whichever is greater, or
>
> **(C)** both such actions. If the court finds that the defendant wilfully or knowingly violated this subsection or the regulations prescribed under this subsection, the court may, in its discretion, increase the amount of the award to an amount equal to not more than 3 times the amount available under subparagraph (B) of this paragraph."

A relevant example of a company that violated this regulation is Papa John's pizza promotion campaign. The Pizza company was sued for sending unsolicited pizza promotion texts and had to pay $16.3 million to settle the class action suit.

CTIA in the US

The Cellular Telecommunications Industry Association (CTIA), a trade association that represents all wireless communication in the US, offers recommendations and guidance for communication over wireless devices. It has recently released new updates on best practices and principles designed to provide enhanced protection of consumers and messaging platforms against spam, fraud and other messaging issues.

The new recommendations continue to increase consumer protection from spam over wireless channels. These updates clarify that:

- Any organization sending text messages to consumers should receive clear, opt-in consent.
- Messages from organizations that have not obtained opt-in consent may be subject to measures that include delaying or blocking messages.
- The updated best practices also include steps and recommendations that organizations should use to avoid messages being caught in spam filters and other platform protections.

CTIA guidance is not a legal requirement for businesses messaging within the US.

Recommendations for US Regulatory Compliance

The best recommendation is to simply take the time to understand and follow the law with no shortcuts. As a baseline minimum, we recommend the following:

- Always capture consent before you text message with anyone. That includes your customers, unless communications consent for all channels (or messaging) is included in your agreements.
- Tie consent to a specific subject matter and Sender ID. That way if someone opts-out to one type of messaging, you have the opportunity to attract them to opt-in to another subject and/or sender.
- Store your consent within the individual records of your CRM or database. Keep a record of that consent in a protected database.
- Track all the conversations you have, both interactive and automated, with each individual. Store that history in your CRM or database record.
- When an individual opts-out, store that opt-out in the record and be sure you block that record from receiving text messages. We also recommend you confirm the opt-out with one final message.

Regulatory Compliance in Canada

The Canadian Anti-Spam Law (CASL) went into effect July 1, 2014. It is enforced by the Canadian Radio-Television and Telecommunications Commission (CRTC.) Messages that are sent within, to, or from Canada fall within CASL's purview. CASL does not apply to CEMs that are only routed through Canada. For any in transit messages, the regulations of the final receiving country are applied.

Here's the full text of the law, if you'd like to dig into the details. The CRTC offers an FAQ page and consent guidelines as well.

Canadian Anti-Spam Legislation (CASL)

The CASL applies to all electronic messages that are sent by companies as part of their business activities. These are known as Commercial Electronic Messages (CEM) and include email and text messages containing coupons or informing customers about a sale or promotion.

CEMs are promotional in nature. Transactional messages, e.g., those containing website URLs or providing company information, are not considered as CEMs.

CASL requires that Canadian and all other global organizations obtain consent from their recipients before sending promotional Commercial Electronic Messages.

Understanding Customer Consent in CASL

The law defines two types of consent: implied and express. Implied consent is a soft interpretation. Express consent requires action from both sender and recipient.

Implied consent includes the following scenarios:

- A recipient has purchased a product, service or made another business deal, contract, or membership with your organization in the last 24 months;
- Your business is a registered charity or political organization, and the recipient has made a donation or gift, has volunteered, or attended a meeting organized by your business; or
- A professional message is sent to someone whose email address was given to your business, or is conspicuously published, and to someone who hasn't published or told you that they don't want unsolicited messages.

If your recipients don't meet any of the above criteria for implied consent, then express consent is required before you can send campaigns to them.

Express consent means written or oral agreement to receive specific types of messages. For example, checking the box next to the following statement on a webform. "You want to receive monthly newsletters and weekly discount notifications from Company B."

Express consent is only valid if the following information is included with your request for consent:

- A clear and concise description of your purpose in obtaining consent,
- A description of messages you'll be sending,
- Requestor's name and contact information (physical mailing address and telephone number, email address, or website URL,)
- A statement that the recipient may unsubscribe at any time.

The requestor can be your business or someone for whom you're asking. If you're requesting consent on behalf of a client, the client's name and contact information must be included with the consent request.

CASL Exemptions

Certain types of CEMs are either fully or partially exempted from meeting the CASL regulations. In general, these exemptions fall on messages that are not used for sales and marketing purposes.

The fully exempted CEMs include:

- CEMs that are sent between family and friends (related through marriage, common law or any legal parent-child relationship, or if there is a voluntary two-way communication between the individuals).
- CEMs that are sent within or between organizations with an existing relationship (B2B).
- CEMs that are sent in response to complaints, inquiries or requests.
- CEMs sent due to a legal obligation or to enforce a right.
- CEMs sent from instant messaging platforms (like BBM messenger, LinkedIn InMail) where the required

identification and unsubscribe mechanisms are clearly published on the user interface.

- CEMs sent from platforms that have limited access, are secure, and are confidential accounts (like banking portals).
- CEMs sent to listed foreign countries, where it is reasonable to believe that the message will be opened in a listed foreign country that has similar rules as CASL.
- CEMs sent by registered charities for the primary purpose of fundraising.
- CEMs sent by political parties seeking contributions.

Partial exemptions are extended to all CEMs that are sent for the first time after receiving a referral to obtain consent for future messages. This assumes that all other factors required for CEMs that are fully exempted are in place. These include:

- CEMs that are sent between family and friends.
- CEMs sent between organizations that share an existing business relationship.
- CEMs being sent display sender details that include the full name of the individual(s) making the referral, the identity of the sender and an unsubscribe mechanism.

All messages sent following the initial message need to comply with the CASL compliance guidelines. In other words, it needs to follow the form and content requirements defined by CASL like sender identification and unsubscribe mechanisms.

CASL Non-Compliance

Non-compliance with CASL risks heavy penalties for your organization. The maximum penalty for an individual is $1 million. The maximum penalty for a business is $10 million.

Additionally, individuals are able to bring a private civil action against the offending party for damages caused. This may result in criminal charges, civil charges, personal liability for company officers and directors. Penalties for violations are to be determined by a judge.

Recommendations for Canadian Regulatory Compliance

The best recommendation is to simply take the time to understand and follow the law with no shortcuts. And since the laws between the US and Canada are similar, so are the recommendations:

- Always capture consent before you text message with anyone. That includes your customers, unless communications consent for all channels (or messaging) is included in your agreements.
- Tie consent to a specific subject matter and sender. That way if someone opts-out to one type of messaging, you have the opportunity to attract them to opt-in to another subject and/or sender.
- Store your consent within the individual records of your CRM or database. Keep a record of that consent in a protected database. If you are hit with a CASL violation, the burden of proof for consent will be on you, so be prepared.
- Track all the conversations you have, both interactive and automated, with each individual. Store that history in your CRM or database record.
- When an individual opts-out, store that opt-out in the record and be sure you block that record from receiving text messages. We also recommend you confirm the opt-out with one final message.

Regulatory Compliance in the European Union

The General Data Protection Regulation (GDPR) is a mandatory compliance law that all individuals and businesses operating within the European Union (EU) and European Economic Area (EEA) must follow. It came into effect on May 25th, 2018, and covers all forms of communications, including telephone, email and text messaging.

GDPR was created to make the data regulations cohesive across the EU member states. It grants individuals increased rights over their personal data and how it is used. GDPR requires that any information is processed lawfully, fairly and transparently. It also dictates that when information is collected, it is explicitly specified what it will be used for and that it is taken for legitimate reasons. Additionally, such information can't be processed again for any other purposes beyond the initial reason.

Additionally, the GDPR includes the following requirements:

- **Any personal data that you keep must come with consent.** Anyone using that personal information must provide an audit trail proving that it was given freely, in an informed way, for a specific purpose(s) and that you are only using it for that purpose(s). Silence, consent for other purposes, or inactivity are not considered as consent.

- **Information must be stored and managed so that recipients can easily review it or request that it be deleted.** You must be able to provide an audit trail evidencing deletion. Subjects can also request specifics on how you are using their data. You must also maintain an audit trail of all communications between your organization and each individual subject.

- **All information must be stored securely and be protected against any unlawful or unauthorized processing.** This also includes protection from hackers or others who might potentially steal and then use personal information.

If your business communicates with EU data subjects, it is critical that your messaging strategy meets GDPR regulations.

Regulatory requirements are growing more strict across the world. For example, the state of California recently passed the California Consumer Protection Act (CCPA) that will go into effect in 2020. The CCPA mirrors GDPR in many ways. We recommend that all of our customers define a compliance policy and process that meets the current GDPR standard to save time, money and protect future communications as regulations evolve.

To read the entire law in its original form, click here.

General Data Protection Regulation (GDPR)

GDPR compliance is mandatory for any business using SMS business text messaging to recipients within the EU, called EU data subjects. Non-compliance consequences include a fine of up to 10% of your company's revenue.

Basic requirements are noted below.

Explicit opt-in

Businesses using SMS messaging need to ensure that they receive an explicit opt-in request from their audience members. This means that a customer or prospect must give you a definitive approval (consent) to send specific types of content to them via text message.

Specific SMS opt-ins

Businesses often use multiple channels for marketing, namely, email, SMS, direct mail and so on. Under GDPR requirements, it is mandatory that customers opt-in for specific individual channels. This negates the previous compliance concept of bundled opt-ins that provided a generic opt-in for all available channels.

Companies are required to maintain specific opt-ins for every individual channel they are utilizing for marketing products or services. Within each channel, specific content types must also be segmented. Companies must obtain consent for each content type within each channel.

Provision to Opt-out / Permission to Withdraw

New GDPR requirements include the requirement to provide easy access to opt-out or remove consent from receiving text messaging communications. Organizations must provide clear and distinct instructions to help recipients understand the different ways in which they can remove consent. Some of the commonly used opt-out mechanisms are subscription centers, checkboxes on forms or keyword responses, such as STOP.

Businesses should regularly share opt-out instructions in easy-to-comprehend language.

Also, alternative locations where recipients can opt-out should be shared at regular intervals. Companies must provide the complete terms and conditions that make it clear how to opt-out of all future SMS messages

Named parties

Companies receiving consent must be explicitly named in the consent capture agreement. This is an additional enforcement that GDPR is pushing over and above the existing practice of making customer details available only to the party to whom permission is granted.

As per PECR regulations, permissions are explicitly granted only to communications received from pre-approved parties, that are related or relevant to the product or service for which the opt-in was sought. The GDPR requirement reinforces this legislation.

Managing personal data

Companies that collect customer data need to secure and manage this data in accordance with GDPR rules. Some important considerations include:

- Ensure your organization has a good understanding, and documented record of, the data and permission to use it.
- Create an audit process for the initial content and all consequent actions, that is secure and protected. This audit trail may be requested by a recipient at any time. Recipients may also request that you delete this trail and provide evidence of its deletion.
- Ensure your process for opt-outs is effective, is followed and meets GDPR requirements, including a confirmation of the opt-out and options to delete data and/or provide an audit trail of all personal data and actions.
- Define a policy for how long personal data is retained, that it is retained necessarily and that it's kept up to date.
- Ensure that data is being held securely, considering both technology and the human factors in data security.
- Establish whether you are a data controller, data processor, or both and that your organization has the correct legal arrangements in place.

The new GDPR legislation enforces a much more strict level of protection for personal data. If you have questions or concerns, we recommend you seek professional advice immediately. The consequences of GDPR non-compliance are severe.

Countries Included in the GDPR Regulations

Several countries are covered under the GDPR regulations. The list is as follows:

- Austria
- Belgium
- Bulgaria
- Croatia
- Republic of Cyprus
- Czech Republic
- Denmark
- Estonia
- Finland
- France
- Germany
- Greece
- Hungary
- Ireland
- Italy
- Latvia
- Lithuania
- Luxembourg
- Malta
- Netherlands
- Poland
- Portugal
- Romania
- Slovakia
- Slovenia
- Spain
- Sweden
- United Kingdom

GDPR Non-Compliance

Non-compliance with GDPR risks heavy penalties for your organization including fines of up to €20 million or 4% of annual global revenue – whichever is greatest.

Recommendations for EU Regulatory Compliance

The best recommendation is to simply take the time to understand and follow the GDPR law with no shortcuts. Here are the baseline recommendations we share with customers:

- Always capture consent before you text message with anyone. That includes your customers, unless communications consent for all channels (or messaging) is included in your agreements. Even then, it's best to capture an Optin, timestamp it and store it in a protected database.
- Tie consent to a specific subject matter and sender. That way if someone opts-out to one type of messaging, you have the opportunity to attract them to opt-in to another subject and/or sender. GDPR requires that you make this connection.
- Track all the conversations and behaviors (keyword response, for example) that occur, both interactive and automated, with each individual. Store that history in a

secure and protected audit trail in your CRM or database record. Be sure that this audit trail is quickly available to produce as evidence if an individual recipient requests it.

- You must also be sure to store all personal data in a secure database, and to protect that data in flight and at rest. All personal data must be included in the audit trail.
- When an individual opts-out, store that opt-out in the record and be sure you block that record from receiving text messages. Confirm the opt-out, timestamp it all and record it in the audit history.
- If requested, be prepared to delete the individual's personal data (as well as audit trail), and provide proof that the data has been completely deleted.

Summary

Text messaging compliance requires that your business meets both regulatory and carrier requirements. Regulatory compliance is demanded by in country laws and comes with fiscal and operational penalties. Carrier compliance* is necessary if you want the carriers to actually deliver your text messages.

Regulatory compliance protects individuals from unwanted communications, aka spam. It also protects personal data from mis-use.

The key things to remember about regulatory compliance, regardless of your geography, are:

- You must have consent to message an individual.
- You must keep a record of this consent.
- You must keep a record of all communications between your business and your recipients.
- The recipient's data must be protected in a secure database and when it is inflight over networks.

When a recipient opts-out, or removes consent, you must honor that request. Beyond that, use common courtesy as your guideline. Don't over communicate and act like a spammer, don't shamelessly self promote, don't be obnoxious and above all, be respectful in your messaging conversations.

*If you want to learn more about carrier requirements, download our guide, How Messaging Works, by, clicking here.

If you'd like to experience global business messaging for yourself, just request a Free Trial by clicking here. You'll receive access to a full production version of SMS-Magic Converse for 7 days, no questions asked.

Or, you can schedule a demo with one of our textperts by clicking here. We'll show you the ins and outs of business text messaging specifically for your geography and industry.