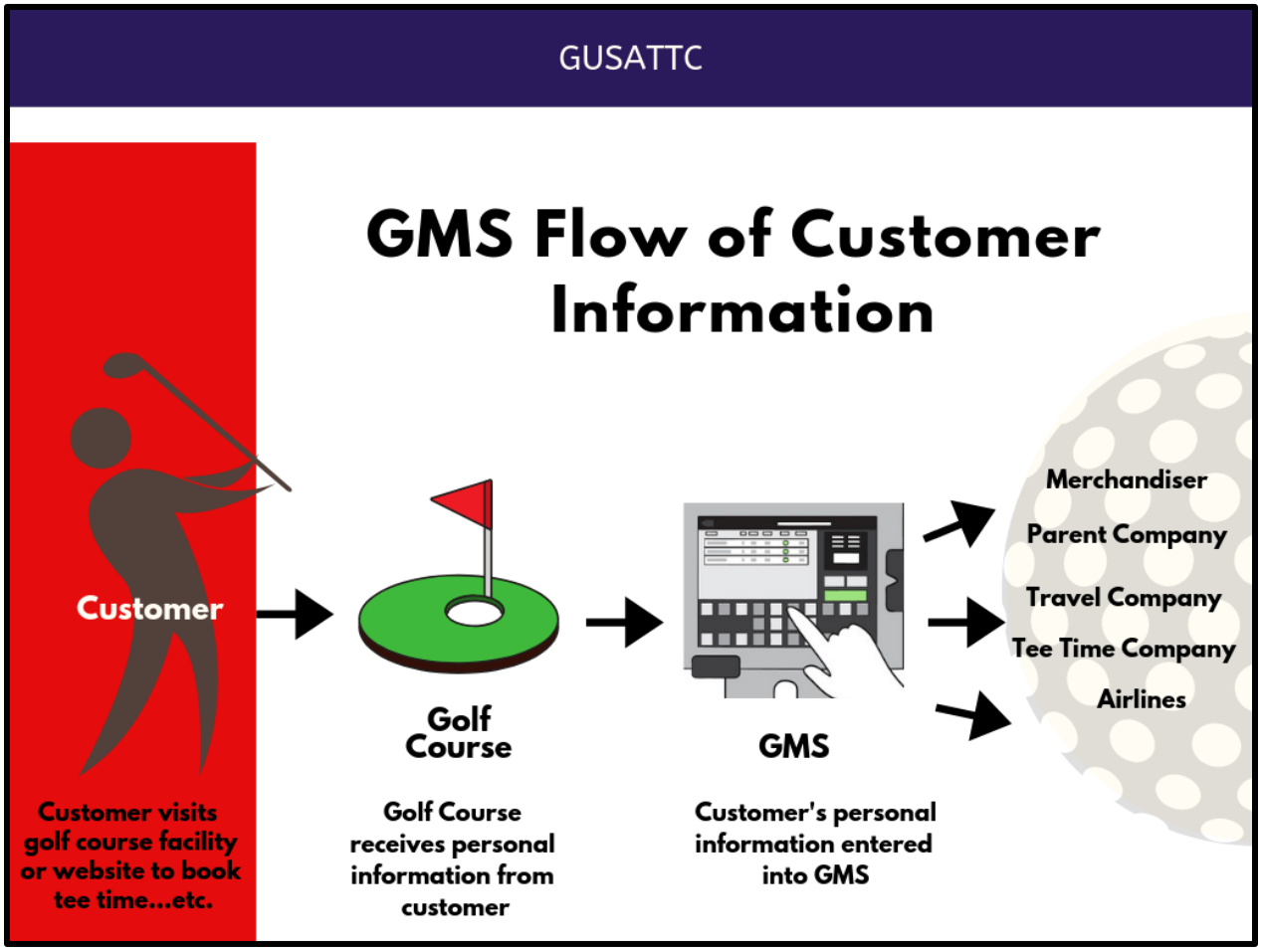
GOLF USA TEE TIME COALITION

Privacy Policy and Email Marketing Best Practices

This document specifically addresses the collection of customer data. However, you (as a golf course owner, operator, or PGA professional) may collect personal information from other persons during the course of your business, including but not limited to: employees, vendors...etc. that may require the implementation of separate data privacy procedures, practices and notices.



Generally speaking, while privacy policies are not expressly required by law, the sum total of rules, regulations and guidelines promulgated by the FTC make it mandatory to disclose to customers how their personal information will be stored, used, shared, sold, licensed, rented, transferred or assigned to third parties if collected through any digital and/or traditional means. This general disclosure to customers is typically delivered by way of a privacy policy. A privacy policy is a legal document or notice that discloses a website owner's practices for collecting, using, maintaining, protecting and/or disclosing the information it gathers through its website from website visitors, users and customers. Because golf course owners and operators collect personal information of customers through POS systems, tee sheets,

subscription based mailing lists and other technologies, platforms or tools, it is important for golf course owner/operators to have a legal mechanism, in the form of a privacy policy, that not only informs customers of what owner/operators do with customer information but also provides owner/operators some protection in the event customer information ends up in the wrong hands.

The following is meant to provide golf course owners and operators with guidance on how to craft, publish, disseminate, update and comply with a legally compliant privacy policy. It also provides tips for complying with applicable email marketing laws, rules, regulations and industry best practices.

PRIVACY POLICY BEST PRACTICES

Disclosures and Notices

There is certain information that must be disclosed in your privacy policy. The following describes what disclosures and additional notices are required in your privacy policy:

- What platforms, tools, applications, websites, companies and collection methods are covered by your privacy policy
- The types of information you collect from customers
- How you use customer information (research, analytics, email marketing, making reservations, etc.)
- How you maintain and store customer information and all measures taken to protect customer information
- Whether or not you sell, share, transfer, assign or disclose ("**Disclosures**") customer information to third parties, the general identities of the third parties and the purpose of any Disclosures
- How you will provide customers with notice regarding any changes you may make to your privacy policy

How to Craft a Privacy Policy Just Right for You

Although most privacy policies include certain general notices, all privacy policies should be uniquely tailored to adequately reflect the data collection processes and procedures of your business. The following is a list of the information that you should collect from key persons within your organization to ensure that the information in your privacy is clearly and accurately stated. If any of the following information is not available or has not yet been determined, make sure to gather and/or determine said information prior to crafting your privacy policy.

- Identify and map out EVERY method, platform and tool used to collect customer data (website, website cookies, digital subscriber lists, tee sheet, POS, sign-up sheet…etc.)
- Identify all third parties who:
    - may have access to your customer information
    - you share customer data with
    - you sell customer data to
- Identify all company uses of customer data
- Identify all storage methods/policies for customer information
- Identify all security measures taken to protect customer information (encryption, firewall, confidentiality policies, limited disclosure…etc.)
- Identify where all customer information is stored (cell phones, laptops, desktops, cloud-based storage…etc.)

Adhering to Your Privacy Policy

Once you have drafted a privacy policy, it is VITAL that you adhere to your policy. Your privacy policy is a contract that obligates you to undertake whatever duties or responsibilities you give yourself pursuant to the policy. Accordingly, it is important to draft a policy that accurately reflects data privacy measures that are not only legally compliant but also operationally feasible for you and your staff. Any failure to adhere to your privacy policy is considered a violation of your self-imposed policy as well as customer trust and may be punishable by law.

Publishing, Posting and Disseminating Your Privacy Policy

The law requires that privacy policies be conspicuously displayed and readily accessible. There is no further guidance regarding what is considered "conspicuous." Most companies display their privacy policies on their websites, regardless of where customer information is collected (online or in-person). The following are recommendations on where privacy policies can be displayed and/or disseminated.

- A notice or link to your privacy policy may be displayed to your user at the time of checkout, if making a purchase online
- An email may be sent to all customers currently on your email list
- You may post your privacy policy on your company website. The privacy policy is generally found in the footer of the website where it is easily accessible from every page on the site.

Making Changes to Your Privacy Policy

You are legally allowed to, and you should, update your privacy policy as often as required for legitimate business purposes and/or to remain compliant with all applicable laws, rules, regulations and/or industry best practices. If you make any changes to your privacy policy, be sure to notify your customers by doing one or more of the following:

- Provide a notice in bold or all caps at the very top of your privacy policy page to make it clear to users that a change has occurred
- Provide a notice in bold, all caps, or via pop-up window on the homepage of your website that clearly states that you have made changes to your privacy policy. You should also include a link to the policy if notice is provided on the home page or via pop-up window
- Send all customers from whom you have collected personal information, an email stating that you have made material changes to your privacy policy. Make sure the email includes a link to the privacy policy and an option to "opt-out" of any further email communication from you.

* Please Note: You are not required to provide notice to customers of any changes to privacy policies of any third parties, even third parties with whom you have shared their personal information.

Providing Clear "Opt-Out" Information

Customers MUST have the option to unsubscribe or "opt-out" from any email marketing or distribution lists you may have. Customers also have the right to request that you delete or remove their personal information from any data collection and/or storage tools that you use. The following are suggestions for providing clear notices, recommendations and/or options for customers who no longer wish to receive communications from you or share information with you.

- In your privacy policy as well as in any email or text message communications, make it clear to customers that they have the option to quickly and easily "opt out" of any communications they receive as a result of information you obtained from them, whether obtained actively or passively.
- Make it easy for customers to unsubscribe by
    - providing an "opt-out" link at the bottom of marketing emails;
    - including a page on your website specifically dedicated to managing customer information and/or email preferences
    - providing contact information and explicit "opt-out" instructions in your privacy policy explaining where customers should direct "opt-out" and personal information removal requests.

BEST PRACTICES FOR CAN-SPAM ACT COMPLIANCE:

If you are collecting customer information, you are most likely sending commercial marketing emails to customers as well. If you are sending commercial marketing emails, make sure that you are in compliance with all laws governing the dissemination of commercial marketing emails.

The Controlling the Assault of Non-Solicited Pornography and Marketing Act (**CAN-SPAM**) regulates the transmission of ALL commercial email messages, not just unsolicited messages. A commercial email message is defined as any email that has a "primary purpose of . . . commercial advertisement or promotion of a commercial product or service" and the act applies to most companies that do business in the U.S. The primary focus is regulating the identification and transmission of unsolicited marketing and sexually explicit e-mails, as well as restricting the gathering and use of personal e-mail addresses.

The following serves to provide guidance on how to comply with the CAN-SPAM Act.

Include on your list only those who want to receive emails

- The mailing list should include only persons who have affirmatively agreed (opted in) to receive commercial email from the business.
- DO NOT email or include on mailing lists customers who have elected to "opt out" of your mailing list.
- Regularly update your mailing list to remove those who have elected to opt out

Make the purpose of your email messages clear

- E-mail header must include complete and accurate transmission information.
- The "From" line must identify the business as the sender. This does not have to include the business's formal name. For example, it may contain the business's name, trade name or product or service name. The key requirement is that the "From" line provide the recipient with enough information to understand who is sending the message.
- The "Subject" line must accurately describe the message's content. If you are selling or advertising goods or services, you don't have to explicitly mention so in the message's subject line, but the subject line should not be intentionally deceptive. (ex: e-mail subject line announcing the arrival of a new head professional and then the content of the e-mail advertising new apparel in the golf shop)
- Include the golf course's valid, current physical postal address.

- If you are selling something, the message must disclose that the email is being sent as an advertisement or solicitation unless the email message is sent ONLY to recipients who have "Opted in" to your mailing list.

Make it EASY for email recipients to Opt-Out

- ALL commercial (emails that sell or advertise goods/services) emails must clearly explain that the recipient may opt out of receiving future commercial messages from your course.
- ALL commercial e-mails must include either an email address or other online mechanism that the recipient may easily use or identify for the purpose of opting out. The mechanism must not require the recipient to:
    - do anything more than reply to the email or visit a single web page to opt out;
    - make any payment or submit any personal information, including account information (other than email address), to opt out; and
    - the opt-out mechanism must work for at least 30 days after the email is sent.
- Ensure that the explanation of how a recipient can opt out is easy to read and understand.
- If you offer "opt out" options that allow customers to reduce the number/type of emails received, one option presented MUST be to "opt out" or unsubscribe from ALL emails.
- Make sure you remove all customers who have "opted out" of your mailing list within ten business days.
- Do not sell, share, or use the private information of any customer who has opted out
- Be diligent in promptly removing customers (no more than 10 business days) from email lists and/or databases once they have elected to opt out of receiving your emails

Managing Customer Data When Dealing With Vendors:

- Make sure you request a copy of any vendor's privacy policy prior to entering into ANY agreement with them
- Review their policy and make sure you understand its terms. You need to know what third parties intend to do with your customer's information.
- Include any pertinent parts of your vendor's privacy policy in your own privacy policy. Make sure that customers know what your third-party vendors may be doing with their sensitive information as well
- Limit the amount access given to vendors of your customer data to what they NEED to know to perform their service, if possible.

Press Contact:
Jared Williams, J.D.
Managing Director
Golf USA Tee Time Coalition
jwilliams@teetimecoalition.org

About the authors

This article was written by Sydnee Mack, Esq. in collaboration with the Golf USA Tee Time Coalition. Sydnee Mack is owner of Sydnee Mack Attorney at Law, a boutique Sports & Entertainment and Small business law firm in Atlanta, GA. Sydnee focuses her sports practice on issues central to the golf community and is also a professor of sports law at the Georgia State University College of Law, also located in Atlanta.