



PRIVACY POLICY

DTC Communications (hereinafter “DTC,” “our,” “us,” or “we”) is committed to respecting and protecting the privacy of our customers. Protecting your private information or Personally Identifiable Information is our priority. This Privacy Policy explains the types of personal information we collect, and how we collect, use, maintain, protect, and share this information. This Privacy Policy also tells you about the rights and choices you may have when it comes to your personal information.

This Privacy Policy applies to the information we collect when you use or interact with our products, services, and networks (“Services”), including <http://www.dtccom.net> (“Website”), but it is not exclusive to it. This Privacy Policy applies to everyone, including, but not limited to, visitors, users, and others who wish to access our Services or Website. By using our Services or Website, you consent to the data practices described in this Privacy Policy.

Please read this Privacy Policy carefully to understand our policies and practices regarding your information.

Definitions

- **Personal Identifiable Information or “personal information”** refers to any information that can be used to identify a specific individual. This includes information that is directly linked to a person, such as their name, date of birth, social security number, or email address, as well as information that can be used to identify them indirectly, such as their physical characteristics, biometric data, or online identifiers like IP addresses or device identifiers.
- **Allowable Tracked Information** refers to the specific types of data that a website or application is permitted to collect, use, and share with third parties. Examples of allowable tracked information that a website or application may collect and use could include: User behavior data, such as website usage patterns, search history, or clickstream data; location data, such as GPS data or IP address; demographic information, such as age, gender, or occupation; contact information, such as email address or phone number; or financial information, such as credit card numbers or payment information.
- **Third Party** refers to any entity that is not directly affiliated with us or our Website that is collecting or processing user data. This can include companies that provide services or products to us, analytics providers, or other third-party service providers. Examples of third parties that may be involved in the collection and processing of user data include:

Analytics providers that collect data on user behavior and provide insights to the organization, or payment processors or financial institutions that process transactions and collect payment information.

- **Cookies** refer to text files placed on a computer, mobile phone, or other device used to navigate the internet. Cookies transmit information back to the website's server about the browsing activities of the user and may also be used to collect and store information about your preferences after you visit a website.
- **Customer Proprietary Network Information (CPNI)** is defined by federal statute to mean: (i) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and (ii) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier.

DTC Obtains and Uses Individual Customer Information for Business Purposes Only

We obtain and use customer information that helps us to provide our customers with quality telecommunications services. In addition to supporting the direct provision of service, this information may be used to protect customers, employees and property against fraud, theft, or abuse; to conduct industry or consumer surveys; and to maintain good customer relations. Access to databases containing customer information is limited to employees who need that information to perform their jobs. These employees are required to follow strict rules when handling customer information and are subject to disciplinary action if they fail to do so.

To better serve our customers, we may ask them questions to elicit additional information about their special needs and interests. For example, we may ask whether customers work at home, whether any members of the household have special needs, or whether teenagers reside in the household to determine whether customers may be interested in or might benefit from additional lines or services. In all cases, the information we gather is used to facilitate the provision of quality customer service. We do not share this information with third parties to market non-DTC services to our customers.

DTC Collects Information from Customers in a Number of Different Ways

We limit the collection, use, retention, and disclosure of personal information to what is reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed. We also limit secondary use to that which is compatible with the original purpose of the personal information collection.

When you visit our Website, you may provide us with two types of information: personal information that you knowingly choose to disclose that is collected on an individualized basis, and website use information collected on an aggregate basis as you and others browse our Website.

You may also be required to provide certain personal information to us when you elect to use certain products or services by (a) registering for an account, (b) entering a sweepstake or contest sponsored by us or one of our partners, (c) signing up for special offers from selected third parties, (d) sending us an email message, and (e) submitting your credit card or other payment information when ordering and purchasing products and services.

We will use your information to communicate with you about services and/or products you have requested from us, including, but not limited to, providing them. We use information about customers in defined and responsible ways to manage, provide, and improve our products, services, and operations for our customers. This information will be used for internal purposes only and will not be shared with any third party. It shall not be used for any improper or unlawful purpose.

We retain customer information for such periods of time as required by law or regulation or as reasonably necessary to provide services.

DTCs E-mail Communications

From time to time, we may contact you via email for the purpose of providing announcements, promotional offers, alerts, confirmations, surveys, and/or other general communication. To improve our services, we may receive a notification when you open an email from us or click on a link therein.

If you would like to stop receiving marketing or promotional communications via email from us, you may opt out of such communications by clicking the “Unsubscribe” button at the bottom of the email.

If you choose to correspond with us through email, we may retain the content of your email messages along with your email address and our responses. We also may send automated messages to you pertaining to your account, such as billing invoices and other notices. We provide the same protections for these electronic communications that we employ in the maintenance of information received by mail or telephone. We ask that you not provide us with confidential information such as social security or account numbers through unsecured email. You may also contact us by phone, U.S. mail, or by visiting our location.

DTC Gives Customers Opportunities To Control Access to Information

We are committed to providing customers with opportunities to control how we use customer information about them. For example, customers may inform us of which telephone listings

they want to include in our directories and in directory assistance and may also choose to have a non-published number, or a non-listed number, or to exclude your address from your listing.

Customers in areas where Caller ID services are available have the ability to block the display of their phone numbers and names. (Note that Caller ID blocking does not prevent the transmission of your phone number when you dial certain business numbers, including 911, or 800, 888, 877, and 900 numbers.) A customer may indicate a change in such preferences at any time by contacting DTC customer service.

We may keep track of the websites and pages our users visit to identify trends among our services. Ordinarily, such information is combined into aggregations that do not include individual customer identities. Under certain circumstances, we are required by law to disclose the aggregated information to other companies, but in such cases, customer identities are not included.

Automatically Collected Information

As you navigate through and interact with our Website, we may use automatic data collection technologies to collect allowable tracked information about your equipment, browsing actions, and patterns, including:

- Details of your visits to our Website, including traffic data, location data, logs, and other communication data, and the resources that you access and use on the Website.
- Information about your device and internet connection, including your IP address, operating system, domain names, access times, and browser type.

We use this allowable tracked information to operate the Website, maintain the quality of the Website, and assess Website usage.

All DTC Employees Are Responsible for Safeguarding Customer Communications and Information

We take reasonable precautions to protect your personal information against unauthorized access. We require all DTC personnel to be aware of and protect the privacy of all forms of customer communications as well as individual customer records. We make it clear that employees who fail to comply with its privacy policies will face disciplinary action, which can include dismissal. All employees are trained regarding their responsibilities to safeguard customer privacy. We strive to ensure that the information we have about our customers is accurate, secure, and confidential and to ensure that our employees comply with our privacy policy.

We never tamper with, intrude upon, or disclose the existence or contents of any communication or transmission, except as required by law or the proper management of our

network. Access to databases containing customer information is limited to employees who need it to perform their jobs – and they follow strict guidelines when handling that information. We use safeguards to increase data accuracy and to identify and authenticate the sources of customer information. We use locks and physical security measures, sign-on and password control procedures, and internal auditing techniques to protect against unauthorized use of terminals and entry into our data systems. We require that records be safeguarded from loss, theft, unauthorized disclosure, and accidental destruction.

In addition, sensitive, confidential, or proprietary records are protected and maintained in a secure environment. It is our policy to destroy records containing sensitive, confidential, or proprietary information in a secure manner. Hard copy confidential, proprietary, or sensitive documents are made unreadable before disposition or recycling, and electronic media must be destroyed using methods that prevent access to information stored in that type of media. Just as employees would report stolen property, missing records and suspicious incidents involving records are referred to DTC Management. We encourage our employees to be proactive in implementing and enforcing DTC's privacy policies. If employees become aware of practices that raise privacy or security concerns, they are required to report them to their supervisors.

Our regulatory team is responsible for ensuring that all DTC business units and their employees comply with privacy laws and regulations. We also require any consultants, suppliers and contractors that may come into contact with customer proprietary information to observe these privacy rules with respect to any of our customers' individual customer information. They must abide by these principles when conducting work for us, and they will be held accountable for their actions.

DTC Takes Special Care to Protect the Safety and Privacy of Young People Using Its Services

We do not provide services to children, and our website is not targeted or marketed to children. We respect the privacy of your children, and we comply with the practices established under the Children's Online Privacy Protection Act. We do not knowingly collect or retain personally identifiable information from children. If you believe that a child has provided their information to us through our Website or Services, please contact us at 615.529.2955 so that we can take steps to delete it.

DTC Complies with All Applicable Privacy Laws and Regulations Wherever DTC Does Business

Customer and policymaker perceptions of privacy have changed over time and will continue to do so. Changes in technology can also alter what is appropriate in protecting privacy. Laws may change accordingly. We regularly examine – and update as necessary – DTC's privacy policies and internal procedures to ensure compliance with applicable law and evolving technology. We also will monitor customer needs and expectations. We will work with policymakers and

consumers to ensure that we continue to safeguard privacy, giving customers choices, flexibility, and control. We consider privacy laws and regulations to be the minimum standards to which we will adhere in protecting privacy. In addition to complying with the law, we will adhere to its internal privacy policies and procedures wherever we do business.

DTC Gives an Authorized Government Agency Access to Customer Information Only Upon Valid Request

We may release customer information in response to requests from governmental agencies, including law enforcement and national security agencies, in accordance with federal statutory requirements or pursuant to court order. Before releasing any customer information, we will ensure that the underlying governmental request satisfies all procedural and substantive legal requirements and is otherwise proper. For example, we will ensure that any court orders are valid, properly issued, and legally enforceable. Except as required by law or with the approval of the customer, DTC will not release any customer information in response to subpoenas or similar requests issued by private parties. Further, we will be diligent in authenticating the validity of any “governmental” request to ensure that the request originates from an authorized government agency.

CPNI Notice

Customers count on us to respect and protect the privacy of information we obtain in the normal course of providing telecommunications services to our customers. We are committed to protecting the privacy of all customer information, and particularly the privacy of customer proprietary network information (or CPNI).

Under federal law, you have the right to, and we have the duty to protect, the confidentiality of your CPNI. However, we may use CPNI without your consent, in a manner consistent with applicable law, to: (i) initiate, render, bill, and collect for our services; (ii) market services among the categories of service to which you already subscribe; (iii) provide inside wiring installation, maintenance, and repair services; (iv) provide maintenance and technical support for our services; (v) protect our rights and property, and protect users of our services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, these services; and (vi) provide any inbound telemarketing, referral, or administrative services for the duration of a customer-initiated call.

To restrict the use of your CPNI data, please contact us at 615.529.2955 to request that we not utilize your CPNI data. Your denial of approval for us to use this data will not affect the provision of any services to which you subscribe. Your approval or denial of approval for the use of CPNI outside of the service to which you already subscribe will remain valid until you revoke or limit the approval or denial.

Limits on the disclosure of CPNI outside DTC

We do not use third-party marketers and will not disclose your CPNI to third party contractors without your explicit “opt in” consent. This means that our records of the services you buy and the calls you make will remain private if you choose to keep them so, since we will not ordinarily disclose this information to outside parties without your permission. However, we will release customer information without involving you if disclosure is required by law, or necessary to protect the safety of customers, employees, or property. For example: When you dial 911, information about your location may be transmitted automatically to a public safety agency. Certain information about your long-distance calls may be transmitted to your long-distance company for billing purposes.

We are also required by law to give competitive local exchange carriers access to customer databases for purposes of serving their customers, to exchange credit information with other carriers, and to provide listings (other than certain non-published and non-listed information) to directory publishers. We will disclose information as necessary to comply with law enforcement statutes, such as to comply with valid, properly issued, and legally enforceable subpoenas, warrants, and court orders. We may, where permitted by law, share CPNI with third parties where necessary to provide the services to which you subscribe, to protect our rights or property, and to protect users of our services and other carriers from fraudulent, abusive, or unlawful use of services. We may, where permitted by law, provide CPNI to third parties such as credit bureaus, or sell receivables to collection agencies, to obtain payment for DTC billed products and services.

Authentication to prevent unauthorized access to CPNI

We are committed to ensuring that only properly authorized individuals are able to access CPNI for legitimate purposes. This includes ensuring that any request by a “customer” to access CPNI is valid and properly authenticated, in accordance with applicable law and industry best practices. In general, our internal policies and procedures are designed to ensure that CPNI is not released to unauthorized individuals.

Further, if a “customer” calls us to access “call detail records” (which include the number called, the number from which a call was placed, and the time, location, or duration of any call), we will not release those records unless (i) during the call, the customer provides a pre-established password; (ii) the information is sent to the customer’s address of record; or (iii) after the call, we call the customer’s telephone number of record to provide the requested information. If a “customer” attempts to access CPNI through our website, we will only provide such access if the customer has first established a password and back-up authentication mechanism for the relevant account, in a manner that does not rely on readily available biographical or account information. If a “customer” attempts to access CPNI by visiting a retail location in person, we will only provide such access if the “customer” presents valid photo identification matching the name of record on the account. (Note that different procedures may apply to certain business customers served by a dedicated account representative where the underlying service agreement addresses CPNI protection and authentication.) We also will notify you at your

address of record if anyone changes the access authorization or authentication information associated with your account.

Notice of unauthorized access to CPNI

We are vigilant in our efforts to protect your CPNI. However, should we become aware that your CPNI has been accessed without proper authority, we will take swift action to fully document and address such unauthorized access and provide appropriate notice. In particular, we will (i) notify law enforcement (including the United States Secret Service and the Federal Bureau of Investigation) within seven business days; and (ii) notify you and any other affected customers within seven business days thereafter, unless earlier notification is necessary to avoid immediate and irreparable harm, or we are instructed by law enforcement personnel to refrain from providing such notice.

National "Do Not Call" List

A National Do-Not-Call Registry has been established to give you an opportunity to help limit the telemarketing calls you receive. Registering your telephone number will restrict commercial telemarketers from calling you. There are some exceptions: businesses with whom you have existing relationships and some non-profit, educational, and political organizations. There is no charge to register your residential telephone number, including wireless numbers on the national Do-Not-Call Registry. You may do so by telephone or via the Internet. To register by telephone, call 1.888.382.1222. For TTY (hearing impaired), call 1.866.290.4236. You must call from the telephone number you wish to register. You may also register via the Internet at www.donotcall.gov. The website also provides additional information.

After you register, your telephone number will show up on the registry within 30 days following your registration. Telemarketers will have up to 31 days to remove your number from their call lists. Your number will remain on the registry for five years, at which time you may re-enter your number on the list. You can remove your name from the list at any time by calling the telephone numbers listed above.

Changes to Our Privacy Policy

We reserve the right to change, modify, or update this Privacy Policy at any time without notice. In the event of any modification, we will post the changes in this Privacy Policy so that you will always know what information we are gathering and how we might use that information. If such changes are material, we will either announce the change on the home page of the site or take such other action as we deem appropriate under the circumstances. Accordingly, you should periodically visit this page to determine the current Privacy Policy to which you are bound.

Contact Information

If you have questions about this Privacy Policy or wish to contact us concerning personal information you provided through the use of our Website, please contact us at the following:

DTC Communications
PO Box 247
Alexandria, TN 37012-0247
615.529.2955