

National Wireless Privacy Policy

Last Updated: January 31, 2023

Summary of Changes Since Last Update (September 21, 2022 version):

- Added Definitions sections in the general Privacy Policy, California/Nevada/Virginia Resident Rights and Notice sections and new Definitions therein;
- Added Electronic Device Identifiers such as “IMEI” (International Mobile Equipment Identity), and “ICCID” (Integrated Circuit Card Identifier) to the “Types of Personal Information We Collect About You” and “Sources of Personal Information We Collect About You” sections;
- Removed the “Your Rights and Our Obligations Related to Your Customer Proprietary Network Information” section and references to Customer Proprietary Network Information (CPNI) throughout;
- Reorganized the “Types of Information We Collect About You” section;
- Updated the “Sources of Personal Information We Collect About You” to include federal, state regulators, and other related third parties;
- Updated the “Your Advertising Choices and Consent Options” to reflect changes to the use of Google Analytics and our Marketing Communications policy;
- Updated the “Our Contact Information” section; and
- Added stylistic changes throughout.

Introduction and Overview

This Privacy Policy (“Privacy Policy”) applies to you and anyone who uses National Wireless’ (“National Wireless,” “we,” “us,” or “our”) Devices, Products, or Services (collectively, “Services”) under your account, except where we identify for you that separate terms and conditions apply. You are responsible for making sure all users under your account understand and agree to this Policy. You are responsible for making sure all users under your account understand and agree to this Policy.

Please take a moment to review the full terms of our Privacy Policy below, because by continuing to access or use our Services, you accept and agree to be bound by all terms of the Privacy Policy. If you do not agree with any portion of it, then you must not access or use our Services. We may change this Privacy Policy from time to time, so check this policy regularly for updates.

This Privacy Policy is part of the Terms and Conditions governing the use of our Services, which can be found at www.natwireless.com. To the extent that any provision or clause in our Terms and Conditions conflicts with any provision or clause in this Privacy Policy or a specific service plan offer, the terms of those more specific documents will govern.

Contents

Definitions

Types of Personal Information We Collect About You

Sources of Personal Information We Collect About You

How We Use Personal Information We Collect About You

How We Share or Allow Access to Your Personal Information

How You Might Share Your Personal Information with Third Parties

Your Advertising Choices and Consent Options

How We Store, Retain, Protect Personal Information We Collect About You, and How Long We Keep Your Personal Information

Governing Law and Notice to Non-U.S. Residents

Information from Children

California Resident Privacy Rights and Notice

Nevada Residents Privacy Rights and Notice

Virginia Residents Privacy Rights and Notice

Changes and Updates to this Privacy Policy

Our Contact Information

Definitions

“Call Detail Information” means any information that pertains to the transmission of specific telephone calls, including, for outbound calls, the number called, and the time, location, or duration of any call and, for inbound calls, the number from which the call was placed, and the time, location, or duration of any call.

“Device” means any phone, smartphone, tablet, accessory, or other device provided or sold to you by National Wireless or that you activate or use with our Services.

“Geolocation Data” means any data that is derived from a device and that is used or intended to be used to locate a consumer within a geographic area.

“Precise Geolocation” means any data that is derived from a device and that is used or intended to be used to locate a consumer within a geographic area that is equal to or less than the area of a circle with a radius of 1,850 feet, except as prescribed by law or regulation.

“Personal Information” is information that identifies you or is reasonably capable of being associated with or linked, directly or indirectly, with you or your household. It does not include aggregate, de-identified, and/or anonymous information that is not reasonably capable of being associated with or linked, directly or indirectly, with you or your household.

“Services” means voice telephony (“talk”), text messaging (“text”), broadband Internet access (“data”), and any other services provided to you by National Wireless, services and devices subject to Affordable Connectivity Program discounts, and prepaid wireless service.

“Underlying Carrier” means the wireless provider whose facilities we use to provide you wireless Services.

Types of Personal Information We Collect About You

Depending on how you interact with us or our Services, we may collect the following categories of Personal Information from or about you, including, for example:

- **Identifiers**, such as your name, address, e-mail address, telephone number, date of birth, internet protocol (“IP”) address, social security number, account name, username(s), social security number, driver’s license number, state identification card number, passport number; cookies and Electronic Device Identifiers such as “IMEI” (International Mobile Equipment Identity), and “ICCID” (Integrated Circuit Card Identifier).
- **Information in customer records** such as your name, address, social security number, driver’s license or state ID card number, passport, phone number, insurance policy number, education, employment, bank account number, financial information.
- **Financial information associated with you** such as such as credit card, debit card, checking account information, purchase and order history, and billing information related to your use of our voice and text services; documentation of participation in an eligible government low-income or financial assistance program, documentation demonstrating proof of income, or your Social Security number, each of which will only be used to determine Affordable Connectivity Program (“ACP”) eligibility.
- **Characteristics of protected classifications under State or Federal law**, such as Tribal status (*i.e.*, National Origin, Ancestry in California) to determine ACP eligibility.
- **Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies**, such as your purchase and order history, frequency of use, and quantity of use, your interaction with our communications and advertisement, broadband usage, and your activity on your Device.
- **Biometric information**, such as interactive voice control communications with our customer service system, and recorded audio interactions with our customer service representatives.
- **Internet or other electronic network activity information**, such as information about your use of the Services, including the date and time of your use, frequency of use, and quantity of use, your interaction with our communications and advertisement, broadband usage, and your activity on your Device; your internet protocol (“IP”) address, browser type, operating system, software version, and Device type, model, and Electronic Device Identifiers (IMEI and ICCID).

- **Geolocation Data**, such as the location of your Device when it is connected to our network and our Underlying Carrier's network.
- **Audio, electronic, visual, thermal, olfactory, or similar information**, such as interactive voice control communications with our customer service system, and recorded audio interactions with our customer service representatives.
- **Professional or employment-related information**, such as employment status.
- **Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. section 1232g, 34 C.F.R. Part 99)**, such as school enrollment information necessary to establish ACP eligibility.
- **Sensitive Personal Information**, such as your social security number, driver's license number, state Identification card number, and/or passport number; your login, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account; and Precise Geolocation, as defined above.
- **Inferences drawn from any of the categories identified above to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes**, such as such as information about your use of the Services, including the date and time of your use, frequency of use, and quantity of use, your interaction with our communications and advertisement, broadband usage, and your activity on your Device.

Sources of Personal Information We Collect About You

We may obtain Personal Information about you in 3 ways:

- **Information You Provide Directly to Us.** You may give us Personal Information, such as Identifiers, Information in customer records, Financial information associated with You, Professional or employment-related information, and Sensitive Personal Information, including when you apply for, subscribe to, or purchase our Services; communicate with us using our contact information; or provide us with your Device when you relinquish, exchange, return, or recycle your Device or provide it to us, our contractors, or our vendors for maintenance.
- **Information We Collect Automatically from You.** We, our service providers, or contractors may automatically or passively collect Personal Information, such as Internet or other electronic network activity information, Geolocation Data, Sensitive Personal Information (Precise Geolocation) when you use or interact with our Services, including through the use of network management technology and third-party analytics and advertising tools, which may use cookies, web beacons, pixel tags, log files, local shared objects (Flash cookies), HTML5 cookies, or other technologies to automatically or passively collect information about your use of and interaction with the Services.
- **Information We Collect from Other Sources.** We may collect any category of Personal Information from affiliates, business partners, federal and state regulators, subsidy program administrators, compliance and service support entities, or third parties (such as social media platforms, data aggregators, public databases, and other commercially available sources), which may include the information you provide those entities or that they automatically collect from you.

We may combine the various types of Personal Information we receive from or about you, including information you provide to us, information we automatically collect, and information from other sources, and use it as described in this Privacy Policy.

How We Use Personal Information We Collect About You

Except as otherwise prohibited by law or regulation, and subject to applicable instructions from you to us, we may use your Personal Information for a variety of business and commercial purposes, including for:

- **Verifying Eligibility and Subscribing You to Our Services.** To verify your identity and eligibility for the ACP and subscribe you to our Services, including to execute requests to port your phone number.
- **Providing, Improving, and Maintaining Our Services.** To provide, improve, and maintain our Services, including to: initiate and render our Services; maintain the accuracy of the information we collect; track, measure, and analyze the usage and operations of our Services; maintain, manage, optimize, and resolve problems with our wireless networks, information technology, and our Services; develop and improve our business, content, products, and Services; and interact with third-party services, at your request.

- **Customer Service.** To respond to questions and comments about your account and Services, to communicate with you about your account status and technical issues, and for training or quality assurance purposes.
- **Billing and Payments.** To complete your purchases, including billing and payment processing, which may involve the use of cookies.
- **Prevention and Detection of Unlawful and Unauthorized Use.** To prevent and detect fraud, abuse, and other unlawful and unauthorized use of our Services, including to investigate possible violations of and enforce our Terms and Conditions and any other contracts, and to otherwise protect the security or integrity of the Services, our business and property, and our rights and interests, and those of you, our other customers, our service providers or contractors, and other businesses.
- **Complying with Legal and Regulatory Obligations.** To comply with our legal and regulatory obligations, including responding to legal process, such as subpoenas, court orders, and search warrants.
- **Emergency Situations.** To allow responses to 911 requests and for other emergencies or exigencies in cases involving danger of death or serious physical injury to you or any other person.

We may use your Personal Information as otherwise disclosed and explained to you at the point of collection and with your consent, where necessary.

How We Share or Allow Access to Your Personal Information

Except as otherwise prohibited by law or regulation, and subject to applicable instructions from you to us, we may share or allow access to your Personal Information for a variety of business and commercial purposes, including, for example:

- **Sharing Across Affiliates.** With our parent, subsidiary, and affiliate companies for business, operational, and legal purposes.
- **Provide, Improve, and Maintain Our Services.** With service providers or contractors that provide business, professional, or technical support functions for us and help us provide, improve, and maintain our Services, such as by administering activities on our behalf, including network operations, website hosting, database management, information technology, billing and payment processing, customer service, analysis of our Services, and the sale and delivery of our Services. Billing and Processing may include the use or sharing of Call Detail Information. Call Detail Information may include Geolocation Data (and Precise Geolocation), such as your location when using our network. We do not authorize service providers or contractors to use or disclose the Personal Information they collect, except as necessary to perform services on our behalf, and require them to protect the confidentiality and security of the Personal Information they receive consistent with this Privacy Policy.
- **Protect Our Services and Users.** With governmental authorities or other entities if we believe disclosure is necessary or appropriate to: protect against fraudulent, malicious,

abusive, unauthorized, or unlawful use of our Services; protect our network, databases, Services, Devices, users, and employees from physical or financial harm; and investigate violations of our Terms and Conditions or other contracts.

- **Legal Rights and Obligations.** With governmental authorities, auditors and third-party identity verification services, credit bureaus or collection agencies, and other entities to the extent necessary to: respond to subpoenas, court orders, search warrants, or other legal process; respond to requests for cooperation from law enforcement or other government entities, including pursuant to the Communications Assistance for Law Enforcement Act (CALEA), which may require that we monitor or facilitate monitoring and otherwise disclose the nature and content of communications transmitted through the Services or Devices without any further notice or liability; comply with legal and regulatory obligations, including identity verification, fraud and identify theft protection, and protection, advancement, or defense of our rights or the rights of others; recover payment for previously-billed Services; and facilitate or verify the appropriate calculation of taxes, fees, or other obligations due to local, state, or federal governments and governmental agencies.
- **Sale or Transfer of Business or Assets.** With our professional advisers in connection with a corporate transaction, such as a sale, assignment, divestiture, merger, bankruptcy, consolidation, reorganization, liquidation, or other transfer of the business or its assets. If another entity acquires National Wireless or any of our assets, your Personal Information may be transferred to such entity. In addition, if any bankruptcy or reorganization proceeding is brought by or against us, such information may be considered an asset of ours and may be sold or transferred to third parties. Should such sale or transfer occur, we will use reasonable efforts to try to require that the buyer or transferee use your Personal Information in a manner that is consistent with this Privacy Policy.
- **Emergencies.** With governmental authorities or other entities or individuals in emergency situations involving danger of death or serious physical injury to you or any other person, to respond to 911 requests, and for other emergencies or exigencies.
- **Commercial Marketing Purposes.** With our affiliates, service providers, contractors, or marketing partners for our marketing and advertising purposes, including when we use our marketing partner's analytic and advertising tools, such as cookies, web beacons, pixel tags, log files, local shared objects (Flash cookies), HTML5 cookies, or other technologies that automatically or passively collect Personal Information from your use of our Services.

We do not and will not sell or knowingly allow third parties unauthorized access to your Personal Information.

How You Might Share Your Personal Information with Third Parties

When using our Services, you may choose to install, access, or use services offered by third parties, such as websites, applications, and the networks of other carriers (such as when you are

roaming). Please also refer to the Acceptable Use Policy inside our Terms and Conditions, available at www.natwireless.com.

When you interact with third-party services, you may be consenting to those third parties accessing, collecting, using, or disclosing your Personal Information through our Services or directing us to share or allow access to your Personal Information by those third parties, such as your IP address, browsing activity, or location information. Those services operate independently of our Services, and your Personal Information will be governed by their terms and conditions, including their privacy policies, not this Privacy Policy. We encourage you to review the privacy policies of any third-party services that you use to better understand their privacy practices. You may be able to restrict or disable the use and disclosure of certain information, such as your location information, using settings available on your Device or through the third-party services.

Your Advertising Choices and Consent Options

Google Analytics and Google AdWords. We may use Google Analytics on our Sites to help us analyze traffic and improve services. For more information on Google Analytics' processing of Personal Information, please see <http://www.google.com/policies/privacy/partners/>. You may opt-out of the use of Google Analytics here: <https://tools.google.com/dlpage/gaoptout>.

Our Sites also use the Google AdWords remarketing service to advertise on third party websites (including Google) to previous visitors to our site. This could be in the form of an advertisement on the Google search results page or a site in the Google Display Network. Third-party vendors, including Google, use cookies to serve ads based on someone's past visits to our Sites. Any data we collect will be used in accordance with this Privacy Policy, and Google is responsible to abide by its own privacy policy. You can set your preferences for how Google advertises to you using the Google Ad Preferences page: <https://adssettings.google.com>.

You have certain choices and consent options related to the use and disclosure of your Personal Information for advertising purposes. Exercising these choices and options will not affect our provision of Services to you. Please note that these choices and options may not prevent you from receiving all advertising; you may continue to receive generic advertising from us or interest-based advertising from third parties, depending on how they operate.

Interest-Based Advertising. You have choices and options concerning interest-based advertising on our Services or across other websites and online services as follows:

- To opt-out of collection and use of your Personal Information for interest-based advertising by companies participating in the Digital Advertising Alliance ("DAA"), please visit optout.aboutads.info or click on the DAA icon when you see it on an online ad.
- To opt-out from the use of Personal Information about your online activities for interest-based advertising by Network Advertising Initiative ("NAI") member companies, please visit optout.networkadvertising.org.

- To opt-out of the use of your mobile device ID for targeted advertising, please visit www.aboutads.info/appchoices.
- To prevent your Personal Information from being used by Google Analytics to measure and improve marketing and advertising and understand the use of our Services, including through Google AdWords, Google Display Network Impression Reporting, DoubleClick Platform Integrations, and Google Analytics Demographics and Interest Reporting, add the Google Analytics opt-out plugin to your browser, available at tools.google.com/dlpage/gaoptout.
- To manage flash cookies, visit Adobe's Global Privacy Settings Panel.
- You may be able to adjust your browser, computer, or device settings to disable cookies, remove or prevent the storage of HTML5, or control other advertising and analytics technology to stop or reduce the amount of interest-based advertising you receive, but doing so may prevent you from using certain features of our Services.

Marketing Communications. In accordance with our Terms and Conditions, you provide consent for us to contact you via email, voice call or text, including manual, autodialed, and prerecorded calls and texts. You may limit or revoke these authorizations as follows:

- Call us at (888) 683-7521.
- Unsubscribe from our email communications following the unsubscribe instructions contained within our emails.
- Reply "STOP" to our text messages.

Your instructions to opt-out from these communications will be processed as soon as reasonably practicable. Please note that exercising a marketing opt-out will not affect the services you receive and will not affect National Wireless's right to contact you about the services to which you subscribe, including notifications regarding compliance obligations related to those services (e.g., non-usage, de-enrollment, and collection notices).

Do Not Track. Because Do Not Track ("DNT") and similar signals do not yet operate according to common, industry-accepted standards, our Services may not respond to DNT signals.

How We Store, Retain, Protect Personal Information We Collect About You, and How Long We Keep Your Personal Information

We maintain reasonable physical, technical, and procedural safeguards to help protect against loss, misuse, or unauthorized access, disclosure, alteration, or destruction of your Personal Information. We encrypt sensitive information (such as financial payment information) and transmissions involving customer accounts. We only retain your Personal Information for as long as reasonably necessary to fulfill the purposes for which we collected it, including for any legal, accounting, or reporting purposes, as well as to resolve disputes and enforce our agreements.

We will keep your Personal Information as long as necessary to provide your Services, or as otherwise required by federal or state law, subpoena, or court order.

FCC regulations require us to keep:

- Affordable Connectivity Program (ACP) records for as long as an ACP participant receives a discount but no less than six (6) years.
- 911 call data for two (2) years.

The Personal Information we collect from or about you is stored on servers which we take commercially reasonable efforts to secure in the United States, subject to the laws of the United States. Electronic access to the databases and physical access to the servers on which this Personal Information is stored are restricted to those employees, agents, contractors, service providers, and other third parties who have a business need for such access. They will only access and use your Personal Information based on our instructions and they are required to keep your Personal Information confidential. While we take reasonable steps to help ensure the integrity and security of our network and servers, we cannot guarantee their security, nor can we guarantee that your communications and information will not be intercepted while being transmitted over our underlying carrier's network or the Internet.

Governing Law and Notice to Non-U.S. Residents

Our Services are solely intended for individuals located within the United States ("U.S.") and its territories and are subject to U.S. law. If you are located outside of the United States and its territories, please do not use the Services.

We may transfer the Personal Information we collect about you to countries other than the country in which the information was originally collected, for the purposes outlined in the How We Share or Allow Access to Your Personal Information section above. Those countries may not have the same data protection laws as the country in which you initially provided the information. When we transfer your information to other countries, we will protect that information as described in this Privacy Policy.

Information from Children

Our Services are not directed toward children, and we do not knowingly collect Personal Information from children under the age of 13 (or under the age of 16 in California).

While you may have supplied information about children under age 13 (or age 16 in California), such as school enrollment or school breakfast/lunch program documentation to qualify for the Affordable Connectivity Program, we do not control or possess that information; that information is held and controlled by the Universal Service Administrative Company (USAC).

If you are a minor, please do not provide us any Personal Information or use or access the Services without receiving your parent's or guardian's permission. If we learn that we have collected any Personal Information from a child under the age of 13 (or under the age of 16 in California), we

will take steps to delete the information as soon as possible. If you believe that we might have any Personal Information from a child under 13 (or under the age of 16 in California), or if you are a parent or guardian of a child under 13 (or under the age of 16 in California) that has provided us with Personal Information without your consent, please contact us at (888) 683-7521 or www.natwireless.com/contact to request deletion of the child's information.

California Resident Privacy Rights and Notice

Individuals residing in California on a permanent basis (California residents) have certain rights described below.

California Civil Code Section 1798.83

Under California's "Shine the Light" law, California residents have the right to request in writing from businesses with whom they have an established business relationship: (a) a list of the categories of Personal Information, such as name, e-mail, mailing address, and type of services provided to the customer, that a business has disclosed to third parties (including affiliates that are separate legal entities) during the immediately preceding calendar year for the third parties' direct marketing purposes; and (b) the names and addresses of all such third parties.

To request this information, please contact us at service@natwireless.com or (888) 863-7521.

California Consumer Protection Act

This section provides additional information for California residents under the California Consumer Privacy Act ("CCPA") and any effective amendments thereto. The terms used in this section have the same meaning as those used in CCPA. This section does not apply to information that is not considered "Personal Information" under CCPA such as anonymous, deidentified, aggregated, or public information. The CCPA defines these terms as:

"Aggregate consumer information" means information that relates to a group or category of consumers, from which individual consumer identities have been removed, that is not linked or reasonably linkable to any consumer or household, including via a device. "Aggregate consumer information" does not mean one or more individual consumer records that have been de-identified.

"De-identified" means information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, provided that a business that uses deidentified information:

- (1) Has implemented technical safeguards that prohibit reidentification of the consumer to whom the information may pertain.

(2) Has implemented business processes that specifically prohibit reidentification of the information.

(3) Has implemented business processes to prevent inadvertent release of de-identified information.

(4) Makes no attempt to reidentify the information

“Personal information” means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following:

(A) Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier Internet Protocol address, email address, account name, social security number, driver’s license number, passport number, or other similar identifiers.

(B) Any categories of personal information described in subdivision (e) of Section 1798.80, i.e., including, but not limited to, his or her name, signature, social security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information. “Personal information” does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(C) Characteristics of protected classifications under California or federal law. California protected classifications include race; color; religion (includes religious dress and grooming practices); sex/gender (includes pregnancy, childbirth, breastfeeding and/ or related medical conditions); gender identity/expression; sexual orientation; marital status; medical condition; military or veteran status; national origin; ancestry; disability (mental and physical including HIV/AIDS, cancer, and genetic characteristics); genetic information; request for family care leave; request for leave for an employee’s own serious health condition; request for pregnancy disability leave; retaliation for reporting patient abuse in tax-supported institutions; age (over 40).

(D) Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.

(E) Biometric information.

(F) Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an Internet Web site, application, or advertisement.

(G) Geolocation data.

(H) Audio, electronic, visual, thermal, olfactory, or similar information.

(I) Professional or employment-related information.

(J) Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. section 1232g, 34 C.F.R. Part 99).

(K) Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes

"Personal information" does not include publicly available information. For these purposes, "publicly available" means information that is lawfully made available from federal, state, or local government records, if any conditions associated with such information. "Publicly available" does not mean biometric information collected by a business about a consumer without the consumer's knowledge. Information is not "publicly available" if that data is used for a purpose that is not compatible with the purpose for which the data is maintained and made available in the government records or for which it is publicly maintained. "Publicly available" does not include consumer information that is deidentified or aggregate consumer information.

"Sell," "selling," "sale," or "sold," means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration.

The CCPA states that a business does not sell personal information when:

(A) A consumer uses or directs the business to intentionally disclose personal information or uses the business to intentionally interact with a third party, provided the third party does not also sell the personal information, unless that disclosure would be consistent with the provisions of this title. An intentional interaction occurs when the consumer intends to interact with the third party, via one or more deliberate interactions. Hovering over, muting, pausing, or closing a given piece of content does not constitute a consumer's intent to interact with a third party.

(B) The business uses or shares an identifier for a consumer who has opted out of the sale of the consumer's personal information for the purposes of alerting third parties that the consumer has opted out of the sale of the consumer's personal information.

(C) The business uses or shares with a service provider personal information of a consumer that is necessary to perform a business purpose if both of the following conditions are met: services that the service provider performs on the business' behalf, provided that the service provider also does not sell the personal information.

(i) The business has provided notice that information being used or shared in its terms and conditions consistent with California Civil Code Section 1798.135.

(ii) The service provider does not further collect, sell, or use the personal information of the consumer except as necessary to perform the business purpose.

Collection and Disclosure of Personal Information

Personal Information Notices. For purposes of compliance with the CCPA, in addition to other details described in this Privacy Policy, we provide the following notices:

- We collect the following categories of Personal Information as described in the Types of Personal Information We Collect About You and Sources of Personal Information We Collect About You sections above
- We disclose the following categories of Personal Information for a business purpose as described above in How We Use Personal Information We Collect About You and How We Share or Allow Access to Your Personal Information.

Retention of Personal Information

We only retain your Personal Information for as long as reasonably necessary to fulfill the purposes for which we collected it, including for any legal, accounting, or reporting purposes, as well as to resolve disputes and enforce our agreements. We outline specific retention periods in the How We Store, Retain, Protect Personal Information We Collect About You, and How Long We Keep Your Personal Information section above.

Purpose of Collection

As explained above in How We Use Personal Information We Collect About You and How We Share or Allow Access to Your Personal Information, we also collect your Personal Information for the following business or other notified purposes:

- Auditing relating to a current interaction with you, including but not limited to counting ad impressions, verifying positioning and quality of ad impressions, and compliance.

- Detecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, and prosecuting those responsible for that activity.
- Debugging to identify and repair errors that impair existing intended functionality.
- Performing services on behalf of ourselves or a service provider or contractor, such as maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, providing advertising or marketing services, providing analytic services, or providing similar services.
- Undertaking internal research for technological development and demonstration.
- Undertaking activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by us, and to improve, upgrade, or enhance the service or device that is owned, manufactured, manufactured for, or controlled by us.

We note that under the CCPA, use of your Personal Information for these purposes is not subject to consumer's Right to Delete, as described below and under California law.

Sale of Personal Information

We do not sell Personal Information as that term is defined under CCPA. If we ever decide to sell Personal Information, we will provide you with notice and a right to opt-out of such sale.

Right to Know

You have the right to request the following about the Personal Information we have collected about you in the past 12 months:

- The categories of Personal Information we collected about you;
- The categories of sources from which the Personal Information was collected;
- The business or commercial purpose for collecting the Personal Information;
- The categories of third parties with whom we shared the Personal Information;
- The categories of Personal Information we disclosed for a business purpose; and
- The specific pieces of Personal Information we collected about you.

To submit a request under your Right to Know, contact us using the information provided below in Exercising Your CCPA Rights. Please note that under California Law, that we are only required to respond to such requests from you twice in a twelve-month period.

Right to Correct Inaccurate Information

Beginning on January 1, 2023, you will have the right to correct inaccuracies in your Personal Information that we have collected, taking into account the nature of the Personal Information and the purposes of processing the Personal Information.

To submit a request under your Right to Correct, contact us using the information provided below in Exercising Your CCPA Rights.

Right to Delete

You have the right to request the deletion of your Personal Information collected or maintained by us, subject to limitations established by federal law, including federal subsidy program enrollment and verification data.

To submit a request under your Right to Delete, contact us using the information provided below in Exercising Your CCPA Rights.

Exercising Your CCPA Rights

To make a request described above, you may contact us at:

service@natwireless.com
(888) 683-7521

Verification and Response Process

General Process

If you submit a request to access, correct, or delete Personal Information, we will need to verify your identity and confirm your request before processing it. When you make such a request, you can expect the following:

- We will verify your identity. You will need to provide us with your email address and full name. We may ask for additional information if needed.
- We will confirm that you want your information accessed, corrected, and/or deleted.
- We will confirm our receipt of your request within 10 days. If you have not received a response within a few days after that, please let us know by contacting us at the phone number or email address listed above.
- We will respond to your request within 45 days. If we need additional time to respond, we will notify you within the original 45 days, and provide a final response within 45 days thereafter. If we need an extension, we will explain why.

Denials

In certain cases, a request to access, correct, or delete may be denied. For example, if we cannot verify your identity, the law requires that we maintain the information, or if we need the information for internal purposes such as providing Services or completing an order.

We may also deny a request for deletion if it is necessary for us or a service provider or contractor to maintain your Personal Information in order to:

- Complete the transaction for which the Personal Information was collected, fulfill the terms of a written warranty or product recall conducted in accordance with federal law, provide a good or service requested by you, or reasonably anticipated within the context of our ongoing business relationship with you, or otherwise perform a contract between us.
- Detect security incidents; protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for that activity.
- Debug to identify and repair errors that impair existing intended functionality.
- Exercise free speech, ensure the right of another customer to exercise their right of free speech, or exercise another right provided for by law.
- Comply with the California Electronic Communications Privacy Act.
- Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the deletion of the information is likely to render impossible or seriously impair the achievement of such research, if you have provided informed consent.
- Enable solely internal uses that are reasonably aligned with your expectations based on our relationship.
- Comply with a legal obligation.
- Otherwise use your Personal Information, internally, in a lawful manner that is compatible with the context in which you provided the information.

If we deny any of your requests, we will explain why we denied it. If there is a portion of your request that we can comply with, for example deleting some of the requested information, then we will do so.

Right to Non-Discrimination

You have a right not to receive discriminatory treatment by us for exercising any of your privacy rights conferred by the CCPA. We will not discriminate against any California consumer because such person exercised any of the consumer's rights under CCPA, including, but not limited to:

- Denying goods or services.
- Charging different prices or rates for goods and services, including through the use of discounts or other benefits or imposing penalties.
- Providing a different level or quality of goods or services.
- Suggesting that you will receive a different price or rate for goods or services or a different level or quality of goods or services.

We may, however, charge a different price or rate, or provide a different level or quality of goods or services, if that difference is related to the value provided by your data.

Authorized Agent

You may designate an authorized agent to make a request under the CCPA on your behalf, using the contact information above. Such requests will still undergo a verification process, and we will deny requests from agents who do not submit proof of authorization from you. To verify that an authorized agent has authority to act for you, we may require a copy of a power of attorney or require that you provide the authorized agent with written permission and verify your own identity with us.

Nevada Residents Privacy Rights and Notice

We comply with applicable requirements of the Nevada privacy law (Nevada Revised Statutes Chapter 603A), which in some instances provides Nevada residents with choices regarding how we use and share your personal information.

Nevada Personal Information (“Nevada PI”) includes personally identifiable information about a Nevada consumer collected online, such as an identifier that allows the specific individual to be contacted. Nevada PI also includes any other information about a Nevada consumer collected online that can be combined with an identifier to identify the specific individual.

We may collect your telephone number in addition to the categories information we outline in the Types of Personal Information We Collect About You section above (which include the Nevada PI categories of first and last name; physical address; email address; and username).

We may share such Personal Information with categories of third parties including federal and state regulators, subsidy program administrators, compliance and service support entities, and marketing entities.

Unaffiliated third parties outside of our control may collect covered information about your online activities over time and across different Internet websites or online services (via , e.g., “cookies”) when you use our Services.

You have the right to request that we not sell your Personal Information. Although we do not currently sell Personal Information, you may submit a request directing us to not sell Personal Information if our practices change in the future. To exercise this right, you may contact us service@natwireless.com or at [mailto:DataRequest@playonsports.com?subject=CCPA%20Request\(888\)683-7521](mailto:DataRequest@playonsports.com?subject=CCPA%20Request(888)683-7521).

Virginia Residents Privacy Rights and Notice

Beginning on January 1, 2023, Virginia residents will have certain additional rights described below, to the extent that we:

- (i) during a calendar year, control, or process Personal Data of at least 100,000 consumers or
- (ii) control or process Personal Data of at least 25,000 consumers and derive over 50 percent of gross revenue from the sale of personal data.

You may inquire whether these thresholds have been met by contacting us at (888) 683-7521 or service@natwireless.com. To the extent the threshold has been met, you may exercise these rights.

Definitions

"Personal Data," for purposes of this section means any information that is linked or reasonably linkable to an identified or identifiable natural person. "Personal Data" does not include de-identified data or publicly available information.

"Precise Geolocation Data" means information derived from technology, including but not limited to global positioning system level latitude and longitude coordinates or other mechanisms, that directly identifies the specific location of a natural person with precision and accuracy within a radius of 1,750 feet. "Precise Geolocation Data" does not include the content of communications or any data generated by or connected to advanced utility metering infrastructure systems or equipment for use by a utility.

"Sale of Personal Data" means the exchange of Personal Data for monetary consideration by National Wireless to a third party. "Sale of Personal Data" does not include:

1. The disclosure of Personal Data to a processor that processes the Personal Data on behalf of National Wireless;
2. The disclosure of Personal Data to a third party for purposes of providing a product or service requested by the consumer;
3. The disclosure or transfer of Personal Data to an National Wireless affiliate;
4. The disclosure of information that the consumer (i) intentionally made available to the general public via a channel of mass media and (ii) did not restrict to a specific audience; or

5. The disclosure or transfer of Personal Data to a third party as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the National Wireless's assets.

"Sensitive data" means a category of Personal Data that includes:

1. Personal Data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status;
2. The processing of genetic or biometric data for the purpose of uniquely identifying a natural person;
3. The Personal Data collected from a known child; or
4. Precise Geolocation data

Virginia Residents are notified of the following:

- The categories of Personal Data processed by National Wireless are listed in the "Types of Personal Information We Collect About You" section above. With respect to Geolocation Data, National Wireless only collects Call Detail Information. As defined by Virginia privacy law, Call Detail Information does not constitute Precise Geolocation data (*i.e.*, "data generated by or connected to advanced utility metering infrastructure systems or equipment for use by a utility.");
- The purpose(s) for processing Personal Data is listed in the How We Use Personal Information We Collect About You above;
- We outline how consumers may exercise their consumer rights and how a consumer may appeal an National Wireless decision with regard to the consumer's request below;
- The categories of Personal Data that National Wireless shares with third parties are listed in the "How We Share or Allow Access to Your Personal Information" above; and
- The categories of third parties with whom we share Personal data are described in the "Information We Collect from Other Sources" paragraph within the "Sources of Personal Information We Collect About You" section above.

Right to Know, Correct, and Delete Under the Virginia Consumer Data Protection Act

To the extent applicable, Virginia provides residents with specific rights regarding Personal Data, including:

- To confirm whether or not we are processing your Personal Data and to access such Personal Data;
- To correct inaccuracies in your Personal Data that we have collected, taking into account the nature of the Personal Data and the purposes of processing the Personal Data;
- To request deletion of Personal Data that we have collected, subject to legal exemptions; and
- To obtain a copy of your Personal Data.

To exercise these rights, you may contact us at service@natwireless.com
<mailto:DataRequest@playonsports.com?subject=CCPA%20Requestor> (888) 683-7521.

Right to Opt Out

To the extent applicable, Virginia residents also have the right to opt out of the processing of Personal Data for purposes of targeted advertising, the sale of Personal Data, or profiling in furtherance of decisions that produce legal or similarly significant effects.

Right to Non-Discrimination

You have the right not to receive discriminatory treatment by us for exercising any of your privacy rights. We will not discriminate against you for exercising any of your rights under this section, including, but not limited to:

- Denying goods or services.
- Charging different prices or rates for goods and services.
- Providing a different level or quality of goods or services.

We may, however, charge a different price or rate, or provide a different level or quality of goods or services, if that difference is related to the value provided by your data and/or your voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program.

Verification and Response Process

If you submit a request to access, correct, or delete Personal Data, we will need to verify your identity and confirm your request before processing it. When you make such a request, you can expect the following:

- We will verify your identity. You will need to provide us with your email address and full name. We may ask for additional information if needed.
- We will confirm that you want your information accessed, corrected, and/or deleted.

- We will confirm our receipt of your request within 10 days. If you have not received a response within a few days after that, please let us know by contacting us at the email or phone number listed above.
- We will respond to your request within 45 days. If we need additional time to respond, we will notify you within the original 45 days, and provide a final response within 45 days thereafter. If we need an extension, we will explain why.
- In certain cases, a request for access, correction, or deletion may be denied. For example, if we cannot verify your identity, the law requires that we maintain the information, or if we need the information for internal purposes such as providing Services or completing an order. If we deny your request, we will explain why we denied it. If there is a portion of your request that we can comply with, for example deleting some of the requested information, then we will do so.

Consumer Request Appeal Process

To the extent applicable, if we deny your request to access, correct, or delete Personal Data, you have the right to appeal that decision using the following process:

- Contact us in the same manner you submitted your original request with the subject line: “Appeal—Virginia Privacy Request.”
- Within 60 days of receipt of your appeal, we will respond and inform you in writing of any action taken or not taken, including a written explanation of the reasons for our decision.
- If we deny your appeal, you may contact the Virginia Attorney General to submit a complaint here: <https://www.oag.state.va.us/consumer-protection/index.php/file-a-complaint>.

Changes and Updates to this Privacy Policy

We reserve the right to modify this Privacy Policy at any time. When we do, we will post the changes on this page. We will give you notice of any materially adverse changes to this privacy policy and may give you notice of all other changes but reserve the right to make such modifications immediately if required. It is your responsibility to regularly check this page to determine if there have been changes to the Privacy Policy and to review such changes.

The most current version of this Privacy Policy can be viewed by visiting our website and clicking on “Privacy Policy” located at the bottom of the pages. Any changes will take effect immediately. The effective date of this Privacy Policy is stated below. Continued access or use of our Services following the effective date of any changes shall indicate your acceptance of such changes. If you

do not agree to the modified provisions of this Privacy Policy, you must discontinue your access and use of the Services.

Our Contact Information

If you have any questions or concerns about this Privacy Policy or how we treat your Personal Information, please contact us using the following information:

Email: service@natwireless.com

Phone: (888) 683-7521 during normal business hours: Monday-Friday 8am to 5pm CST.