PRIVACY POLICY

Download | REGIONAL SUPPLEMENTS | Prior Version

Xanterra Leisure Holding, LLC, along with its subsidiary companies listed below (collectively "Xanterra," "us," "our," or "we"), is committed to respecting your privacy. This Privacy Policy ("Privacy Policy") describes how we collect, process, and share your Personal Data (defined below). We also describe your rights and choices with respect to your Personal Data and other important information. Please read this Privacy Policy carefully.

SCOPE OF THIS POLICY

This Privacy Policy applies to Personal Data collected through our "Services", which include:

- Our "Offline Services" – Services you use when you visit properties or travel with companies operated by Xanterra;
- Our "Digital Services" – Our websites, mobile applications, and other online services, including data collected when you interact with or reference our products/services or advertisements online.

Note that certain third parties may be able to identify you across sites and services using the information they process; however, any such processing not done at the direction of Xanterra is outside the scope of this Privacy Policy. This Privacy Policy does not apply to Personal Data collected in the employment context or for other HR purposes, all of which is covered by our HR Privacy Notice.

WHO WE ARE

Xanterra Leisure Holding, LLC is a Colorado-based company with offices at 6312 S. Fiddlers Green Cir., Ste. 600 North, Greenwood Village, Colorado 80111. Its subsidiary companies include, at the time of publication of this Privacy Policy: Xanterra Holding Corporation; Xanterra Leisure Resort Holding, LLC; Xanterra Parks & Resorts, Inc.; Xanterra South Rim, L.L.C.; GCR Acquisitions, LLC; Grand Canyon Railway, LLC; Grand Canyon Railway Hotel, LLC; Xanterra Tusayan, LLC; Xanterra Cedar Creek, LLC; Xanterra Adventure Companies, LLC; Holiday Vacations, LLC; Xanterra Cruise, LLC; Otago France; Windstar Cruises Marshall Islands, LLC; and Windstar Cruises, LLC.

HOW TO CONTACT US/CONTROLLER

The controller of your Personal Data under this Policy is Xanterra Leisure Holding, LLC. If you have any comments or questions about this Privacy Policy or privacy practices, please contact our Data Privacy Team at:

Xanterra Leisure Holding, LLC
Attn: Privacy
6312 S. Fiddlers Green Cir., Ste. 600 North
Greenwood Village, CO 80111

General Inquiries and Data Updates: preferences@xanterra.com

Marketing Choices: If you would like to make changes to your communications preferences with regard to any Xanterra entity, click the link in any email from the applicable Xanterra entity to change your preferences with regard to that entity, or send us an email at preferences@xanterra.com and let us know to which Xanterra entity your request is related.

Data Rights: to exercise your data rights (access, deletion, correction) with regard to a particular Xanterra entity, visit the Data Request Portal on the privacy policy page accessed from that Xanterra entity's website or call 1-844-388-2813.

Opt-Out of Data Sales and Sharing (for advertising purposes), Limit Sensitive Data Use/Processing: to opt out of data sales and sharing (as defined by applicable data privacy laws) with regard to a particular Xanterra entity, you may either visit our Privacy Choices

Commented [HD1]: I moved this to the bottom.

Commented [HD2]: Link

Commented [HD3]: Add link

Portal to opt-out for the Xanterra entity from which you have accessed this privacy policy, click the "Your Privacy Choices" link from that entity's website, or in the US call 1-844-388-2813.

Commented [HD4]: Add link

Direct Marketing Disclosure Requests: please email datarequests@xanterra.com.

CATEGORIES AND SOURCES OF PERSONAL DATA

The following describes how we process data relating to identified or identifiable individuals and households ("**Personal Data**").

Categories of Personal Data We Process

The categories of Personal Data we process may include:

Audio/Visual Data- Recordings and images collected from our surveillance cameras when you visit our properties and locations and areas adjacent to them, as well as audio files and records, such as voice mails, call recordings, and the like.

Biographical Data-Data relating to professional and employment history, qualifications, and similar biographic information.

Transaction Data-Information about the Services we provide to you and about reservations and transactions you make with Xanterra or other companies operating through us or on our behalf (including travel agents), information relating to operations or services at our properties and locations you visit, information about purchases and the method of payment you have used for purchases (including gift card purchase and use), what has been provided to you, when and where and, if applicable, how much you paid, and similar information.

Contact Data-Identity Data that relates to information about how we can communicate with you, such as email, phone numbers, physical addresses, social media handles, and information you provide to us when you contact us by email or when you communicate with us via social media.

Device / Network Data- Browsing history, search history, and information regarding your interaction with a web site, mobile application, or advertisement (e.g., IP Address, MAC Address, SSIDs or other device identifiers or persistent identifiers), online user ID, device characteristics (such as browser/OS version), web server logs, application logs, browsing data, first party cookies, third party cookies, web beacons, clear gifs and pixel tags, as well as similar information collected when you use Wi-Fi at our properties or on our ships.

Identity Data-Information such as your name; address; email address; telephone number; date of birth, account login details, including your user name and password, license plate number, or other account-related information; your identity, public profile, and similar information from social networks; and information such as unique IDs and similar data collected or derived from the use of RFID enabled products such as keycards.

Inference Data-Personal Data used to create a profile about you reflecting your preferences, characteristics, behavior, and market segments, likes, favorites and other data or analytics provided about you or your account by social media companies or data aggregators, including household data such as income, number of children, occupation, home ownership status, the products and services you use or intend to use or purchase, and your interests.

General Location Data- Non-precise location data, such as dates and times of your visit, which properties or locations you visited, and location specified by social media tags/posts.

Sensitive Personal Data- Personal Data deemed "sensitive" under various privacy laws, such as social security, driver's license, state identification card, or passport number; account log-in and password, financial account, debit card, or credit card number; precise location data; racial or ethnic origin, religious or philosophical beliefs, etc. We may collect (either directly or through third parties who may provide the data to us) the following categories of Sensitive Personal Data:

- "**Government ID Data**" relates to official government identification, such as driver's license or passport numbers, including similar Identity Data protected as Sensitive Data under applicable law.

- "**Health Data**" includes information about your health, temperature, or vaccinations, or other health-related information you may provide in connection with your bookings. Please note that "Consumer Heath Data," typically defined by applicable state health privacy laws as "personal information linked or reasonably linkable to a consumer and that identifies the consumer's past, present, or future physical or mental health status," is described in and subject to our Consumer Health Data Privacy Policy.
- "**Payment Data**" includes information such as bank account details, payment card number and other payment card data, and information from credit reference agencies, including similar data as defined in applicable law, and relevant information in connection with a financial transaction.
- "**Precise Location Data**" relates to data from GPS, Wi-Fi triangulation, certain localized Bluetooth beacons, mobile devices, or technologies used to locate you at a precise location and time.

User Content-Unstructured/free-form data that may include any category of Personal Data, e.g., data that you give us in free text fields such as comment boxes, answers you provide when you participate in sweepstakes, contests, votes and surveys, including any other Personal Data which you may provide through or in connection with our Services.

Sources of Personal Data We Process

We collect Personal Data from various sources, which include:

Data you provide us-We receive your Personal Data when you provide them to us, when you purchase our products or services, or complete a transaction via our Services, when you purchase or use one of our gift cards, or when you otherwise use our Services.

Data we collect automatically-We collect Personal Data about or generated by any device you have used to access our Services, the websites of any service provider used to purchase accommodations at properties or travel with companies operated by Xanterra, or when you use Wi-Fi at any of our properties or while traveling with companies operated by us.

Service Providers & Agents-We receive Personal Data from on-line travel agents such as Expedia or booking.com or brick and mortar travel agents who transfer Personal Data to us when you purchase accommodations or services from them in connection with Services that we provide, and other service providers performing services on our behalf.

Aggregators and advertisers-We receive Personal Data from ad networks, behavioral advertising vendors, market research companies, data brokers, and social media companies or similar companies that provide us with additional Personal Data such as Inference Data.

Social media companies-We receive Personal Data from Meta (e.g. Facebook and Instagram) and other social media companies who may transfer Personal Data to us when you register for one of our Services or interact with that social media company on or in connection with our services, properties or locations.

Data we create or infer-We, certain partners, social media companies, and third parties operating on our behalf create and infer Personal Data such as Inference Data or Aggregate Data based on our observations or analysis of other Personal Data processed under this Policy, and we may correlate this data with other data we process about you. We may combine any Personal Data about you that we receive from you, from other companies within our family of companies, and from third parties.

DATA PROCESSING CONTEXTS / NOTICE AT COLLECTION

Note: please click the following links to view information on Data Retention or Regional Data Rights for any of the processing contexts listed below.

Purchases and Transactions

We process Identity Data, Transaction Data, Payment Data, Inference Data, Device/Network Data, and Contact Data when you engage in a purchase and sale transaction, whether through our Digital Services or in person, and whether for our products, our services, our gift cards, or

Commented [HD5]: Add link.

otherwise. If provided, we also process Health Data (such as your requests for health-related accommodations, or as otherwise necessary in connection with your visit – please see "Health Data" below) and Government ID Data.

We process this Personal Data as necessary to perform or initiate a contract with you, process your order and payment, carry out fulfillment and delivery, track the use and balance of gift cards, and for our Business Purposes. We may process Identity Data, Transaction Data, Preference Data, Contact Data, and Device/Network Data for Commercial Purposes (which may include data sales/sharing). We do not sell or "share" (for behavioral advertising purposes) Payment Data, Government ID Data, or Health Data or use it for Business Purposes not permitted under applicable law.

Third party businesses/controllers may receive your information. Third Party data controllers/businesses (such as service providers) provide many products and services you purchase through our Services. We may disclose Identity Data, Transaction Data, Contact Data, and Device/Network Data to those third parties. You may also direct us to disclose this data to or interact with these third parties as part of visiting our properties or making a purchase (which does not involve a data sale by us).

Marketing Communications

We process Device/Network Data, Contact Data, Identity Data, and Inference Data in connection with marketing communications, push notifications, telemarketing, or similar communications, and when you open or interact with those communications. You may receive marketing communications if you consent and, in some jurisdictions, as a result of account registration or a purchase.

We process this Personal Data to contact you about relevant products or services and for our Business Purposes. We may use this data for our Commercial Purposes (which may include data sales/sharing). Marketing communications may also be personalized as permitted by applicable law, but will not involve Targeted Advertising where users have opted out or not provided necessary consents. See your Rights & Choices to limit or opt out of this processing.

Visiting our properties or traveling with companies operated by Xanterra

Generally

We process Identity Data, Transaction Data, and Contact Data when you visit our properties or travel with Xanterra. Additionally, if you use electronic or RFID technologies, or use on-premise Digital Services, we will collect Device/Network Data (see below for additional information regarding our Digital Services). In some cases, we will collect Health Data as may be needed in connection with your travel and activities (please also see "Health Data" below) and Government ID Data for identification purposes and in connection with regional requirements. In some situations, when you travel with a Xanterra entity, we may recommend that you use certain mobile applications. Certain mobile applications may feature the branding of a Xanterra entity but are operated for us by third parties, or in other cases the mobile applications may be entirely those of third parties.

We may process Identity Data, Transaction Data, Contact Data, Inference Data, and General Location Data as necessary to operate our properties and provide our services to you, for our Business Purposes, and our other legitimate interests, including:

- verifying your identity for authentication and security purposes;
- helping us to ensure our customers are genuine and to prevent fraud;
- notifying you via email or SMS regarding changes in circumstances impacting your visit; and
- to help us to return lost property to its rightful owner.

We may also use Identity Data, Commercial Data, Contact Data, and Race or Ethnic Origin Data collected in this context for Commercial Purposes. We do not sell or "share" (for behavioral

advertising purposes) Payment Data, Government ID Data, Health Data, Race or Ethnic Origin Data, or use this data for Business Purposes not permitted under applicable law.

Third parties operating mobile applications on our behalf may collect or process Precise Location Data if you have permitted the collection of such data from your mobile device.

Health Data

In certain cases, we process Health Data (for a description of how we process Consumer Health Data, please review our Consumer Health Data Privacy Policy). Health Data, such as your vaccinations, temperature, data on health screening questionnaires, and/or your COVID-19 testing status, may be required (by us or by various laws, regulations, or local authorities) in order to book or embark on some of our offerings, visit certain properties we manage, or visit certain locations at which our cruise ships or tours may stop. Health Data is also used so that we can provide certain services to you such as to provide you with tailored services (for example, a wheelchair accessible space or a sign language interpreter) or in connection with our response to health-related incidents that may have taken place at properties or while traveling with companies operated by Xanterra. Health Data may also be required in connection with certain activities. In addition, we or our third party service providers may collect Health Data if you visit a health clinic on our ships.

Commented [HD6]: Add link.

Where we collect Health Data, we will use it only as necessary to fulfill or ensure compliance with relevant booking contracts, to protect the health, safety, and vital interests of our personnel, guests and the public, to provide healthcare services you may request (where available), and as otherwise necessary for authorized Business Purposes. In each case, where consent is required by law, we will process this information only with appropriate consent. We do not sell or "share" (for behavioral advertising purposes) Health Data or use it for Business Purposes not permitted under applicable law.

CCTV Data

We may process Audio/Visual Data in connection with CCTV or security cameras on and adjacent to properties and facilities managed by Xanterra. We process this data as necessary to operate our CCTV systems, for our Business Purposes, and our other legitimate business interests, such as:

- preventing and detecting crime and to keep people who visit and work at our company locations safe and secure;
- recording and investigating health and safety and other incidents which have happened or may have happened at properties or while traveling with companies operated by Xanterra;
- counting the numbers of people who visit our properties and to analyze flows of people around the properties and facilities for safety and commercial purposes using software which analyzes CCTV camera images; and
- creating aggregate data.

We do not sell or "share" (for behavioral advertising purposes) Audio/Visual Data collected in this context.

Digital Services

Generally

We process Device/Network Data, Contact Data, Identity Data, General Location Data, and Inference Data when you use our Digital Services. You may also be able to complete purchases, sign up as a travel advisor, or enroll in marketing communications through our Digital Services. We may process Precise Location Data through certain Digital Services if you consent. Location Data may be required in order for you to use certain features of our Digital Services. Please note: in some situations, Precise Location Data may be collected by a third party mobile

application recommended by Xanterra, and in some circumstances, the data may be owned and controlled by that third party rather than Xanterra.

We use this Personal Data as necessary to operate our Digital Services, such as keeping you logged in, delivering pages, etc., for our Business Purposes, and our other legitimate interests, such as:

- enhancing the security of our websites, mobile applications and other technology systems;
- analyzing the use of our Services, including navigation patterns, clicks, etc. to help understand and make improvements to the Services, to provide directions and contextual information to you, and other features that require the use of location. This may include the use of "session capture" or "session replay" software, which we use to understand how users are interacting with our websites, and to help us make decisions regarding design and functionality. Third party service providers operating this software may capture this data on our behalf.
- creating aggregate information about users' location and patterns, which we use to help improve our Services.

We may process this Personal Data for our Commercial Purposes (which may include data sales/sharing). You have the right to limit our use of Precise Location Data by withdrawing consent to or disabling the collection of Precise Location Data.

Cookies, Pixels, and Other Tracking Technologies

We process Identity Data, Device/Network Data, Contact Data, Inference Data, and General Location Data, in connection with our use of cookies and similar technologies on our Digital Services. We may collect this data automatically.

We and authorized third parties may use cookies and similar technologies for the following purposes:

- for "essential" purposes necessary for our Digital Services to operate (such as maintaining user sessions, CDNs, and the like);
- for "functional" purposes, such as to enable certain features of our Digital Services (for example, to allow a customer to maintain a basket when they are shopping at an online store);
- for "analytics" purposes and to improve our Digital Services, such as to analyze the traffic to and on our Digital Services (for example, we can count how many people have looked at a specific page, or see how visitors move around the websites when they use them, to distinguish unique visits/visitors to our Digital Services, and what website they visited prior to visiting our websites, and use this information to understand user behaviors and improve the design and functionality of the websites);
- for "retargeting," Targeted Advertising, or other advertising and marketing purposes, including technologies that process Inference Data or other data so that we can deliver, buy, or target advertisements which are more likely to be of interest to you; and
- for "social media" e.g. via third-party social media cookies, or when you share information using a social media sharing button or "like" button on our Services or you link your account or engage with our content on or through a social networking website such as Facebook or Twitter.

We may also process this Personal Data for our Business Purposes and Commercial Purposes (which may include data sales/sharing). See your Rights & Choices for information regarding opt-out rights for cookies and similar technologies. You may implement your preferences with regard to cookies and similar tracking technologies by visiting the Cookie Preferences Page for the Xanterra entity website from which you have arrived at this Privacy Policy.

Commented [HD7]: Add link to cookie preferences page

Third parties may view, edit, or set their own cookies or place web beacons on our websites. We, or third party providers, may be able to use these technologies to identify you across platforms, devices, sites, and services. Third parties may engage in Targeted Advertising using this data. Third parties have their own privacy policies and their processing is not subject to this Policy.

Contests and Promotions

We collect and process Identity Data, Contact Data, and User Content as necessary to process your contest or promotion entry, notify you if you have won, deliver a prize, for our Business Purposes, or other legitimate purposes, such as:

- verifying your identity for authentication and security purposes (in which case we may process Government ID Data to complete verification);
- to improve our Services and to create a personalized user experience; and
- helping us to ensure entries are genuine and to prevent fraud.

We may process Identity Data, Contact Data, and User Content information for our Commercial Purposes (which may include data sales/sharing).

Some programs and offers are operated/controlled by our third-party partners or their affiliates or partners. We may receive this data from third parties to the extent allowed by the applicable partner; otherwise, this Privacy Policy will not apply to data processed by third parties.

Your Personal Data may be public. If you win a contest/sweepstakes, we may publicly post some of your data. We do not post Personal Information without consent where required by law. See any program agreement(s) or terms and conditions for additional details and terms.

Contact Us; Support

We collect and process Identity Data, Contact Data, and User Content when you contact us, e.g. through a contact-us form, or for support. If you call us via phone, we may collect Audio/Visual data from the call recording. We will also collect Health Data if you choose to provide it within a "contact us" email or a support call or email.

We process this Personal Data to respond to your request, and for our Business Purposes. If you consent or if permitted by law, we may use Identity Data and Contact Data to send you marketing communications and for our Commercial Purposes (which may include data sales/sharing).

Account Registration

We process Identity data, Biographical Data, Contact Data, and User Data when you sign up for an account on our Services, e.g. as a user, or as a domestic or international travel advisor. We may also process Device/Network Data and Inference Data.

We process this Personal Data as necessary to perform or initiate a contract with you, pay your commission, or for our Business Purposes. We may process Identity Data, Inference Data, Contact Data, and Device/Network Data for Commercial Purposes, such as personalized marketing communications.

Vendor and Service Provider Applications

We process Identity Data, Contact Data, Government ID Data, Biographical Data, Inference Data, User Content, Payment Data, and Health Data in connection with your application or engagement as a vendor or service provider for Xanterra.

We process this Personal Data as necessary to evaluate, establish, and maintain the vendor relationship, and for our Business Purposes. We do not sell or share Personal Data processed in this context. We process Sensitive Personal Data only for the Business Purposes provided under applicable law, or only with your consent, to the extent is required by applicable law.

Feedback and Surveys

We process Identity Data, Contact Data, Inference Data, and User Content collected in connection with guest surveys or questionnaires.

We process this Personal Data as necessary to respond to guest requests/concerns, for our Business Purposes, and other legitimate interests, such as:

- analyzing guest satisfaction; and
- to allow our third-party partners to communicate with guests.

We may process this Personal Data for our Commercial Purposes (which may include data sales/sharing). We may share Feedback/Survey data relating to third-party partners with those partners, who may use it for their own purposes.

Posts and Social Media

We process Identity Data, Inference Data, Contact Data, and User Content you post (e.g. comments, forum and social media posts, etc.) on our Digital Services. We also process Identity Data, Contact Data, and User Content if you interact with or identify us, the properties where we provide our Services, or other partners on social media platforms (e.g. if you post User Content that engages with or tags our official accounts.)

We process this Personal Data for our Business Purposes, and Commercial Purposes (which may include data sales/sharing).

Posts may be public, or reposted on our Services. Content you provide may be publicly-available when you post it on our Services, or in some cases, if you reference, engage, or tag our official accounts.

PROCESSING PURPOSES

Business Purposes

We and our Service Providers process Personal Data we hold for numerous business purposes, depending on the context of collection, your Rights & Choices, and our legitimate interests. We generally process Personal Data for the following "Business Purposes."

Service Provision and Contractual Obligations

We process Personal Data as necessary to provide our products and Service, to authenticate users and their rights to access the Service and as otherwise necessary to fulfill our contractual obligations to you, and provide you with the information, features, and services you request. Similarly, we may use Personal Data as necessary to audit compliance, and log or measure aspects of service delivery (e.g., to document ad impressions).

Internal Processing and Service Improvement

We may use any Personal Data we process through our Services as necessary in connection with our legitimate interests in improving the design of our Services, understanding how our Services are used or function, for customer service purposes, for internal research, technical or feature development, to track service use, quality assurance and debugging, audits, and similar purposes.

Security and Incident Detection

We may process any Personal Data we collect in connection with our legitimate business interest in attempting to ensure that our properties and locations are secure, identify and prevent crime, prevent fraud, and ensure the safety of our guests. Similarly, we process Personal Data on our Digital Services as necessary to detect security incidents, protect against, and respond to malicious, deceptive, fraudulent, or illegal activity. We may analyze network traffic, device patterns and characteristics, maintain and analyze logs and process similar Personal Data in connection with our information security activities.

Personalization

We process certain Personal Data as necessary in connection with our legitimate business interest in personalizing our Digital Services. For example, aspects of the Digital Services may be customized (including through your Profile) to you so that it displays your name and other appearance or display preferences, to display content that you have interacted with in the past,

or to display content that we think may be of interest to you based on your interactions with our Digital Services and other content. This processing may involve the creation and use of Inference Data relating to your preferences.

Aggregated Data

We process Personal Data about our customers and users in order to identify trends (to create aggregated and anonymized data about our customers/users, buying and spending habits, use of our Services, and other similar information ("Aggregated Data"). We may pass Aggregated Data to the third parties referred to in the section below to give them a better understanding of our business and to bring you a better service. Aggregated Data that does not contain Personal Data is not subject to this Privacy Policy.

Compliance, Health, Safety, Public Interest

We may also process any Personal Data as necessary to comply with our legal obligations, such as where you exercise your rights under data protection law and make requests, for the establishment and defense of legal claims, or where we must comply with our legal obligations, lawful requests from government or law enforcement officials, and as may be required to meet national security or law enforcement requirements or prevent illegal activity. We may also process data to protect the vital interests of individuals, or on certain public interest grounds, each to the extent allowed under applicable law. Please see the How We Share Personal Data section for more information about how we disclose Personal Data in extraordinary circumstances.

Other Business Purposes

If we process Personal Data in connection with our Service in a way not described in this Privacy Notice, this Privacy Notice will still apply generally (e.g., with respect to your rights and choices) unless otherwise stated at collection. We will process such information in accordance with the notice provided at the time of collection or in a manner that is necessary and proportionate to achieve the operational purpose for which the personal information was collected or processed or for another operational purpose that is compatible with the context in which the personal information was collected.

Commercial Purposes

We and certain third parties process Personal Data to further our commercial or economic interests ("Commercial Purposes,") depending on the context of collection and your Rights & Choices.

Please Note – We may require your consent, or we may not engage in processing of Personal Data for Commercial Purposes in some jurisdictions. See the "REGIONAL SUPPLEMENTS" section below for more information.

Consumer Profiles

In order to understand our customers' preferences, and better recommend products and services that are personalized to our customers, we may create a "Consumer Profile" by linking together and analyzing Personal Data collected in the following contexts:

- Purchases and transactions
- Visiting properties or travel with companies operated by Xanterra
- Digital Services
- Contests and promotions
- Contact us; support
- Feedback and surveys

We may also augment Consumer Profiles with Personal Data that we create (such as Inference Data) or that we receive from our subsidiary companies or third parties, and may include Personal Data such as information about Services you have used or purchased previously, information about when you have visited our properties or locations in the past and what

activities you participated in, and demographic data (which may, in some cases, include Race or Ethnic Origin data we have received from third parties).

We use Consumer Profiles to better understand our customers, and for our legitimate interests in market research and statistical analysis in connection with the improvement of our Services. For example, we may analyze the Personal Data of customers who have made a reservation for a particular itinerary in the past and compare them with other people in our database. If we identify customers in the database who have similar Personal Data to other guests, we may then target marketing about a similar offering to the new customer we have identified, for example by sending marketing emails. We may conduct the profiling and send the direct marketing emails automatically. We may also use this information for other Commercial Purposes. Consumer Profiles involve processing that is automated, in whole or in part.

Personalized Marketing Communications

We may personalize Marketing Communications based on your Consumer Profile. If consent to Consumer Profiling or Targeted Advertising is required by law, we will seek your consent.

Targeted Advertising

In some jurisdictions, Xanterra, and certain third parties operating on or through our Services, may engage in advertising targeted to your interests based on Personal Data that we or those third parties obtain or infer from your activities across non-affiliated websites, applications, or services in order to predict your preferences or interests ("Targeted Advertising"). This form of advertising includes various parties and service providers, including third party data controllers, engaged in the processing of Personal Data in connection with advertising. These parties may be able to identify you across sites, devices, and over time.

The parties that control the processing of Personal Data for Targeted Advertising purposes may create or leverage information derived from Personalization, Consumer Profiles, and Marketing Communications. In some cases, these parties may also develop and assess aspects of a Consumer Profile about you to determine whether you are a type of person a company wants to advertise to, and determine whether and how ads you see are effective. These third parties may augment your profile with demographic and other Inference Data, and may track whether you view, interact with, or how often you have seen an ad, or whether you purchased advertised goods or services.

We generally use Targeted Advertising for the purpose of marketing our Services and third-party goods and services, to send marketing communications, including by creating custom marketing audiences on third-party websites or social media platforms. This may involve sharing limited data regarding our customers with social media platforms or other websites in order to determine which of their users appear to have interests or traits similar to our existing customers.

Data "Sales" and "Sharing"

We may engage in "sales" or "sharing" of data as defined by applicable law. For example, we may "sell" certain Personal Data when we engage in marketing campaigns with or on behalf of third party partners, or we may sell, "share" for behavioral advertising purposes, or grant access to Personal Data to our marketing partners and other advertisers in relation to Targeted Advertising, joint promotions, and other marketing initiatives. See the California Rights & Disclosures section for a list of categories of Personal Data sold or shared.

DISCLOSURE/SHARING OF PERSONAL DATA

We may share Personal Data with the following categories of third-party recipients and/or for the following reasons:

Xanterra Companies- we will share your Personal Data internally within our family of companies, as well as any other current or future affiliated entities, subsidiaries, and parent

companies of Xanterra in order to streamline certain business operations, and in support of our Business Purposes, and Commercial Purposes.

Service Providers- We may share your Personal Data with service providers who provide certain services or process data on our behalf in connection with our general business operations, product/service improvements, to enable certain features, and in connection with our (or our Service Providers') Business Purposes. These service providers may include, among others, companies that help us with our marketing campaigns, website functionality (including session capture/replay technology), mobile applications, and other services. We also share Health Data with third party service providers who help to manage health clinics on our ships.

Advertisers, and Social Media Platforms- We may share certain Personal Data with social media platforms, advertisers, ad exchanges, data management platforms, or sponsors in support of our Commercial Purposes. We may allow these third parties to operate on our Services.

Partners, Excursions & Local Providers-Where allowed by law, or with your consent, we will share your Personal Data with providers of related services, e.g. for excursions, tours, or other third party services operated at certain properties or in relation to our Services. You may also direct us to disclose this data to or interact with these third parties as part of your stay with us or use of our Services (which does not involve a data sale by us). However, in other cases, these parties may also receive data for Commercial Purposes and in connection with Data Sales. If you receive medical treatment on one of our ships or if you are in need of healthcare treatment while at one of our locations, we may in some cases, as permitted by law, disclose your applicable information to local providers of healthcare services as necessary for your care.

Public Disclosure- If you use any social media plugin, API, or other similar feature, use a branded hashtag or similar link, or otherwise interact with us or our Services via social media, we may make your post available on our Services or to the general public. We may share, rebroadcast, or redisplay Personal Data or other information in the post to the extent permitted by the relevant social media service.

Data Aggregators- We may share Personal Data with data aggregators in support of our Commercial Purposes and in connection with Data Sales/Sharing. These disclosures/sales can help better personalize our Services, the services of third parties, enrich Consumer Profiles, and help ensure that you see advertisements that are more relevant to your interests.

Successors-We may share Personal Data if we go through a business transition, such as a merger, acquisition, liquidation, or sale of all or a portion of our assets. For example, Personal Data may be part of the assets transferred, or may be disclosed (subject to confidentiality restrictions) during the due diligence process for a potential transaction.

Lawful Recipients-In limited circumstances, we may, without notice or your consent, access and disclose your Personal Data, any communications sent or received by you, and any other information that we may have about you to the extent we believe such disclosure is legally required, to prevent or respond to a crime, to investigate violations of our Terms of Use, in the vital interests of us or any person (such as where we reasonably believe the use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of any individual or to public health or safety,) or in such other circumstances as may be required or permitted by law. These disclosures may be made to governments that do not ensure the same degree of protection of your Personal Data as your home jurisdiction. We may, in our sole discretion (but without any obligation), object to the disclosure of your Personal Data to such parties.

INTERNATIONAL TRANSFERS OF YOUR PERSONAL DATA

Although we generally process data in the United States, if you are located outside the US, or if you book an activity with us outside the US, we may transfer or process your Personal Data in the US, UK, European Economic Area (EEA), and other jurisdictions where Xanterra or our service providers operate. Where required by local law, we ensure your data remains protected in connection with any international transfers. In cases where we transfer Personal Data to jurisdictions that have not been determined to provide "adequate" protections by your home jurisdiction, we will put in place appropriate safeguards to help ensure that your Personal Data are properly protected and processed only in accordance with applicable law. Those safeguards

may include the use of the Data Privacy Framework (see below), EU standard contractual clauses, reliance on the recipient's Binding Corporate Rules program, or requiring the recipient to certify to a recognized adequacy framework. See the "REGIONAL SUPPLEMENTS" section below for more information on our legal bases for processing Personal Data and other disclosures for specific jurisdictions.

EU-U.S. Data Privacy Framework, UK Extension, and Swiss-U.S. Data Privacy Framework

Xanterra Leisure Holding, LLC ("Xanterra") and Xanterra's US subsidiaries listed below ("US Subsidiaries" comply with the EU-U.S. Data Privacy Framework (EU-U.S. DPF), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) as set forth by the U.S. Department of Commerce. Xanterra and the US Subsidiaries have certified to the U.S. Department of Commerce that they adhere to the EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) with regard to the processing of personal data received from the European Union in reliance on the EU-U.S. DPF and from the United Kingdom (and Gibraltar) in reliance on the UK Extension to the EU-U.S. DPF. Xanterra and the US Subsidiaries have certified to the U.S. Department of Commerce that they adhere to the Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) with regard to the processing of personal data received from Switzerland in reliance on the Swiss-U.S. DPF. If there is any conflict between the terms in this privacy policy and the EU-U.S. DPF Principles and/or the Swiss-U.S. DPF Principles, the Principles shall govern. To learn more about the Data Privacy Framework (DPF) program, and to view our certification, please visit https://www.dataprivacyframework.gov/.

Xanterra and the US Subsidiaries are responsible for the processing of personal data they receive, under the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF, and subsequently transfer to a third party acting as an agent on their behalf. Xanterra and the US Subsidiaries comply with the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF Principles for all onward transfers of personal data from the EU, UK, and Switzerland, including the onward transfer liability provisions.

The Federal Trade Commission has jurisdiction over Xanterra's and the US Subsidiaries' compliance with the EU-U.S. Data Privacy Framework (EU-U.S. DPF), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF).

In compliance with the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF, Xanterra and the US Subsidiaries commit to refer unresolved complaints concerning our handling of personal data received in reliance on the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF to JAMS, an alternative dispute resolution provider based in the United States. If you do not receive timely acknowledgment of your DPF Principles-related complaint from us, or if we have not addressed your DPF Principles-related complaint to your satisfaction, please visit https://www.jamsadr.com/DPF-Dispute-Resolution for more information or to file a complaint. The services of JAMS are provided at no cost to you.

For complaints regarding EU-U.S. DPF, UK Extension to the EU-U.S. DPF, and Swiss-U.S. DPF compliance not resolved by any of the other DPF mechanisms, you have the possibility, under certain conditions, to invoke binding arbitration. Further information can be found on the official DPF website: https://www.dataprivacyframework.gov/s/article/ANNEX-I-introduction-dpf?tabset-35584=2.

Xanterra's US Subsidiaries participating in the Data Privacy Framework include the following: Xanterra Holding Corporation; Xanterra Leisure Resort Holding, LLC; Xanterra Parks & Resorts, Inc.; Xanterra South Rim, L.L.C.; GCR Acquisitions, LLC; Grand Canyon Railway, LLC; Grand Canyon Railway Hotel, LLC; Xanterra Tusayan, LLC; Xanterra Cedar Creek, LLC; Xanterra Adventure Companies, LLC; Holiday Vacations, LLC; Xanterra Cruise, LLC; and Windstar Cruises, LLC.

YOUR RIGHTS & CHOICES

You may have certain rights and choices regarding the Personal Data we process. Please note, these rights may vary based on the country or state where you reside, and our obligations under applicable law. See the following sections for more information regarding your rights/choices in specific regions:

- US States/California
- EEA/UK/Switzerland/Other Countries
- Australia

Your Rights

You may have certain rights and choices regarding the Personal Data we process. See the "REGIONAL SUPPLEMENTS" section below for rights available to you in your jurisdiction. To submit a request, contact our Data Privacy Team.

Verification of Rights Requests

If you submit a request, we typically must verify your identity to ensure that you have the right to make that request, reduce fraud, and to ensure the security of Personal Data. If an agent is submitting the request on your behalf, we reserve the right to validate the agent's authority to act on your behalf.

We may require that you match personal information we have on file in order to adequately verify your identity. If you have an account, we may require that you log into the account to submit the request as part of the verification process. We may not grant access to certain Personal Data to you if prohibited by law.

Your Choices

Marketing Communications

You can withdraw your consent to receive marketing communications for a specific Xanterra entity by clicking on the unsubscribe link in an email from that entity, by responding with "OPT-OUT," STOP, or other supported unsubscribe message (for SMS), or by adjusting the push message settings for mobile apps using your device operating system (for push notifications). You can also withdraw your consent to receive marketing communications or any other consent you have previously provided to us by contacting us. To opt-out of the collection of information relating to email opens, configure your email so that it does not load images in our emails.

Withdrawing Your Consent/Opt-Out

You may withdraw any consent you have provided at any time. The consequence of you withdrawing consent might be that we cannot perform certain services for you, such as location-based services, personalizing or making relevant certain types of advertising, or other services conditioned on your consent or choice not to opt-out.

Precise Location Data

You may control or limit Precise Location Data that we collect through our Services by changing your preferences in your device's location services preferences menu, through your choices regarding the use of Bluetooth, WiFi, and other network interfaces you may use to interact with our Services, or, to the extent such data is collected through a mobile app, by changing your consent or related settings within that app. However, please note that use of RFID technologies may be necessary for certain features of our Services. We may still collect general location data even if you opt out of the collection of Precise Location Data.

Cookies, Pixels, Similar Technologies, and Targeted Advertising

General- If you do not want information collected through the use of cookies or pixels, you can manage/deny cookies, pixels, and similar technologies using your browser's settings menu or the Cookie Preferences page for the Xanterra entity website from which you have arrived at this Privacy Policy. You may need to opt out of third-party services directly via the third party. For example, to opt-out of Google's analytic and marketing services, visit Google Analytics Terms of Use, the Google Policy, or Google Analytics Opt-out.

Commented [HD8]: Add link

Targeted Advertising- You may opt out or withdraw your consent to Targeted Advertising by visiting our Privacy Choices Portal. In some cases, you may be able to opt-out by submitting requests to third party partners, including for the vendors listed below:

Commented [HD9]: Add link

- Google Ads
- Facebook Custom Audience Pixel
- Twitter Audience Pixel
- Digital Advertising Alliance's opt-out
- Network Advertising Initiative opt-out

Global Privacy Control (GPC)- Our Digital Services may support certain automated opt-out controls, such as the Global Privacy Control ("GPC"). GPC is a specification designed to allow Internet users to notify businesses of their privacy preferences, such as opting-out of the sale/sharing of Personal Data. To activate GPC, users must enable a setting or use an extension in the user's browser or mobile device. Please review your browser or device settings for more information regarding how to enable GPC.

Please note: We may not be able to link GPC requests to your Personal Data in our systems, and as a result, some sales/sharing of your Personal Data may occur even if GPC is active. See the "REGIONAL SUPPLEMENTS" section below for more information regarding other opt-out rights.

Do-Not-Track - Our Services do not respond to your browser's do-not-track request.

DATA SECURITY

We implement and maintain commercially reasonable security measures to secure your Personal Data from unauthorized processing. While we endeavor to protect our Services and your Personal Data unauthorized access, use, modification and disclosure, we cannot guarantee that any information, during transmission or while stored on our systems, will be absolutely safe from intrusion by others.

CHILDREN

Our Services are neither directed at nor intended for use by persons under the age of 13 in the US, or under the age of 13 to 16 in the EEA, UK, Switzerland, Cayman Islands, or 15/16 in Australia. Further, we do not knowingly collect Personal Data from minors. If we learn that we have inadvertently done so, we will promptly delete it. Do not access or use the Services if you are not of the age of majority in your jurisdiction unless you have the consent of your parent or guardian.

DATA RETENTION

We retain Personal Data for so long as it is reasonably necessary to achieve the relevant processing purposes described in this Privacy Policy, or for so long as is required by law. What is necessary may vary depending on the context and purpose of processing. We generally consider the following factors when we determine how long to retain data (without limitation):

- Retention periods established under applicable law;
- Industry best practices;
- Whether the purpose of processing is reasonably likely to justify further processing;
- Risks to individual privacy in continued processing;
- Applicable data protection impact assessments;

- IT systems design considerations/limitations; and
- The costs associated continued processing, retention, and deletion.

We typically retain Government ID Data and Health Data for so long as you are receiving relevant Services from us (e.g. the duration of your stay or travels). However, we may need to retain such data for longer periods based on legal requirements, other business needs related to your travel, or in connection with incidents during your travel.

We will review retention periods periodically and may pseudonymize or anonymize data held for longer periods.

THIRD PARTY WEBSITES AND MOBILE APPLICATIONS

Except for processing by our service providers (described below), this Privacy Policy does not apply to third party websites, products, or services. For example, we handle some purchases on our Services directly, and third party businesses manage others. Third parties may operate or develop some Xanterra websites and mobile apps, may operate or host a contest/sweepstakes on our Services. In these cases, the terms, conditions, and privacy practices of the third party, not those of the Xanterra, may govern your transactions, and we may have no control over the Personal Data collected.

CHANGES TO OUR POLICY

We may change this Policy from time to time. We will post changes on this page. We will notify you of any material changes, if required, via email or notices on our Digital Services. Your continued use of our Services constitutes your acknowledgement of any revised Policy.

REGIONAL SUPPLEMENTS

US States/California & Others

US State & California Privacy Rights & Choices

Under the California Consumer Privacy Act ("**CCPA**") and other state privacy laws, residents of California and certain other US states may have the following rights, subject to regional requirements, exceptions, and limitations:

Confirm- Right to confirm whether we process your Personal Data.

Access/Know- Right to request any of following: (1) the categories of Personal Data we have collected, sold/shared, or disclosed for a commercial purpose; (2) the categories of sources from which your Personal Data was collected; (3) the purposes for which we collected or sold/shared your Personal Data; (4) the categories of third parties to whom we have sold/shared your Personal Data, or disclosed it for a business purpose; and (5) the specific pieces of Personal Data we have collected about you.

Portability- Right to request that we provide certain Personal Data in a common, portable format.

Deletion- Right to delete certain Personal Data that we hold about you.

Correction- Right to correct certain Personal Data that we hold about you.

Opt-Out (Sales, Sharing, Targeted Advertising, Profiling)- Right to opt-out of the following:

- If we engage in sales of data (as defined by applicable law), you may direct us to stop selling Personal Data.
- If we engage in Targeted Advertising (aka "sharing" of personal data or cross-context behavioral advertising,) you may opt-out of such processing.
- If we engage in certain forms of "profiling" (e.g. profiling that has legal or similarly significant effects), you may opt-out of such processing.

Revoke Consent for Use of Sensitive Personal Data- If we are collecting, using or otherwise processing your Sensitive Personal Data solely based on consent you have provided, you may

revoke that consent at any time. Please note that we only use Sensitive Personal Data where necessary and in accordance with the specific purposes authorized by applicable law, subject to your consent where required. For California residents, because we do not process Sensitive Personal Data for purposes other than those listed in CCPA section 7027(m), the right to limit use of Sensitive Personal Data is not applicable.

Opt-in/Opt-out of Sale/Sharing of Minors' Personal Data- To the extent we have actual knowledge that we collect or maintain personal information of a minor under age 16 in California, those minors must opt in to any sales/sharing of personal information (as defined under CCPA), and minors under the age of 13 must have a parent consent to sales/sharing of personal information. All minors have the right to opt-out later at any time.

Non-Discrimination- California residents have the right to not to receive discriminatory treatment as a result of your exercise of rights conferred by the CCPA.

List of Direct Marketers- California residents may request a list of Personal Data we have disclosed about you to third parties for direct marketing purposes during the preceding calendar year.

Remove Minors' User Content- Residents of California under the age of 18 can delete or remove posts using the same deletion or removal procedures described above, or otherwise made available through the Services. If you have questions about how to remove your posts or if you would like additional assistance with deletion you can contact us. We will work to delete your information, but we cannot guarantee comprehensive removal of that content or information posted through the Services.

Other- To review rights you may have pursuant to state health privacy laws, please review our Consumer Health Data Privacy Policy.

Commented [HD10]: Add link.

Submission of Requests

You may submit requests to a specific Xanterra entity, as follows (please review our verification requirements section). If you have any questions or wish to appeal any refusal to take action in response to a rights request, contact us at datarequests@xanterra.com. We will respond to any request to appeal within the period required by law.

Access/Know, Confirm Processing, Portability, Deletion, and Correction	• You may visit our Data Request portal (applicable to the specific Xanterra entity listed on the portal page) • You may call us at: 1-844-388-2813. You will be directed to leave a voicemail where you will provide your email address, phone number and address we have on file, along with your request. • You may send mail to our Contact Us address above with your email address, phone number and address we have on file, along with your request.
Opt-Out of Sales, Sharing, Targeted Advertising or Profiling, Opt-in/Opt-out of Sale/Sharing of Minors' Personal Data	• You may visit our Privacy Choices portal (applicable to the specific Xanterra entity listed on the portal page) • You may call us at: 1-844-388-2813. You will be directed to leave a voicemail where you will provide your email address, phone number or address, along with your request. • You may send mail to our Contact Us address above with your email address, phone number or address on file, along with your request. • Note: Digital Services supporting GPC (or similar standards) will treat the request as a request to opt-out of Targeted Advertising/sharing on the device where the GPC setting is active.

Commented [HD11]: Add link

Commented [HD12]: Link

Revoke Consents Previously Granted; List of Direct Marketers; Remove Minors' User Content	• Contact us via email to our privacy team at datarequests@xanterra.com

Categories of Personal Data Disclosed for Business Purposes

For purposes of the CCPA, we have disclosed to Service Providers for "business purposes" in the preceding 12 months the following categories of Personal Data, to the following categories of recipients:

Category of Personal Data		Category of Recipients
Audio/Visual Data		**Error! Reference source not found.**; Service Providers; Partners, Excursions & Local Providers; Successors; Lawful Recipients
Biographical Data		
Transaction Data		
General Location Data		
Inference Data		**Error! Reference source not found.**; Service Providers; Partners, Excursions & Local Providers; Data Aggregators; Successors; Lawful Recipients
Device/Network Data		
Contact Data		**Error! Reference source not found.**; Service Providers; Partners, Excursions & Local Providers; Public Disclosure; Data Aggregators; Successors; Lawful Recipients
Identity Data		
Sensitive Personal Data	Gov. ID Data	**Error! Reference source not found.**; Service Providers; Partners, Excursions & Local Providers; Successors; Lawful Recipients; Contact Us/Support
	Health Data	
	Payment Data	**Error! Reference source not found.**; Service Providers; Successors; Lawful Recipients
	Precise Location Data	

Categories of Personal Data Sold, Shared, or Disclosed for Commercial Purposes

For purposes of the CCPA, we have "sold" or "shared" in the preceding 12 months the following categories of Personal Data to the following categories of recipients:

Category of Personal Data	Category of Recipients
Contact Data	Advertisers, and Social Media Platforms; Data Aggregators
Device/Network Data	
Identity Data	
Inference Data	
General Location Data	

Categories of Sensitive Personal Data Used or Disclosed

For purposes of CCPA, we use, and may disclose as described above, the following categories of Sensitive Personal Data: Government ID Data; Health Data; Payment Data; Precise Location Data. However, we do not sell or "share" (for behavioral advertising purposes) Sensitive Personal Data. We do not use these categories of Sensitive Personal Data for purposes other than those listed in CCPA section 7027(m).

EEA/UK/Switzerland/Other Countries

Controller

The controller of Personal Data is: Xanterra Leisure Holding, LLC, 6312 S. Fiddlers Green Cir., Ste. 600N, Greenwood Village, CO 80111.

Rights & Choices

Residents of the EEA, UK, Switzerland, and certain other countries may have the following rights. Please our review verification requirements. Applicable law may provide exceptions and limitations to all rights.

Access-You may have a right to access the Personal Data we process.

Rectification-You may correct any Personal Data that you believe is inaccurate.

Deletion-You may request that we delete your Personal Data. We may delete your data entirely, or we may anonymize or aggregate your information such that it no longer reasonably identifies you.

Data Export-You may request that we send you a copy of your Personal Data in a common portable format of our choice.

Restriction -You may request that we restrict the processing of personal data to what is necessary for a lawful basis.

Objection-You may have the right under applicable law to object to any processing of Personal Data based on our legitimate interests. We may not cease or limit processing based solely on that objection, and we may continue processing where our interests in processing are appropriately balanced against individuals' privacy interests. In addition to the general objection right, you may have the right to object to processing:

- for Profiling purposes;
- for direct marketing purposes (we will cease processing upon your objection); and
- involving automated decision-making with legal or similarly significant effects (if any).

Regulator Contact-You have the right to file a complaint with regulators about our processing of Personal Data. To do so, please contact your local data protection or consumer protection authority.

Submission of International Data Requests

- **Access, Rectification, Data Export, Deletion, Restriction, or Correction:** please visit our Data Request PortalL (applicable to the specific Xanterra entity listed on the portal page).
- **Restriction; Do Not Sell:** please visit our Privacy ChoicesL Portal (applicable to the specific Xanterra entity listed on the portal page).
- **For other questions or requests, please** Contact us via email to our privacy team at datarequests@xanterra.com.

Commented [HD13]: Link

Commented [HD14]: Link

Lawful Basis for Processing

Legal Basis	**Description of Basis & Relevant Purposes**	**Relevant Contexts / Purposes / Disclosures**
Performance of a contract	The processing of your Personal Data is strictly necessary in the context in which it was provided, e.g. to perform the agreement you have with us, to provide products and services to you, to open and maintain your user accounts, to deliver ticket(s) you have purchased, or process requests.	Contexts • Contexts where Personal Data (excluding Sensitive Personal Data) is processed for purposes listed below • Cookies, Pixels, and Other Tracking Technologies (strictly necessary) Purposes • Service Disclosures

		• Partners, Excursions & Local Providers; • Public Disclosure
Legitimate interests	This processing is based on our legitimate interests. For example, we rely on our legitimate interest to administer, analyze and improve our Services and related content, to operate our business including through the use of service providers and subcontractors, to send you notifications about our Services or products you have purchased, for archiving, recordkeeping, statistical and analytical purposes, and to use your Personal Data for administrative, fraud detection, audit, training, security, or legal purposes. See the Business Purposes of Processing section above for more information regarding the nature of processing performed on the basis of our legitimate interests.	<u>Contexts</u> • Contexts where Personal Data (excluding Sensitive Personal Data) is processed for specified legitimate interests or purposes listed below <u>Purposes</u> • We process Personal Data as necessary to provide our products and Service, to authenticate users and their rights to access the Service and as otherwise necessary to fulfill our contractual obligations to you, and provide you with the information, features, and services you request...Similarly, we may use Personal Data as necessary to audit compliance, and log or measure aspects of service delivery (e.g., to document ad impressions). • We process Personal Data as necessary to provide our products and Service, to authenticate users and their rights to access the Service and as otherwise necessary to fulfill our contractual obligations to you, and provide you with the information, features, and services you request. Similarly, we may use Personal Data as necessary to audit compliance, and log or measure aspects of service delivery (e.g., to document ad impressions). • Internal Processing and Service Improvement • Security and Incident Detection • Personalization • Aggregated Data • Consumer Profiles

		• Personalized Marketing Communications <u>Disclosures</u> • Service Providers • Partners, Excursions & Local Providers • Advertisers, and Social Media Platforms • Data Aggregators • Successors • Lawful Recipients
Consent	This processing is based on your consent. You are free to withdraw any consent you may have provided, at any time, subject to your rights/choices, and any right to continue processing on alternative or additional legal bases. Withdrawal of consent does not affect the lawfulness of processing undertaken prior to withdrawal.	<u>Contexts</u> • Contexts where Personal Data is processed for purposes listed below • Cookies, Pixels, and Other Tracking Technologies (except strictly necessary) • Processing of Sensitive Personal Data • Marketing Communications <u>Purposes</u> • Targeted Advertising • Data "Sales <u>Disclosures</u> • Advertisers, and Social Media Platforms
Compliance with legal obligations	This processing is based on our need to comply with legal obligations. We may use your Personal Data to comply with legal obligations to which we are subject, including to comply with legal process. See the Business Purposes of Processing section above for more information regarding the nature of processing performed for compliance purposes.	<u>Business Purposes</u> • Compliance, Health, Safety, Public Interest <u>Disclosures</u> • Lawful Recipients • Partners, Excursions & Local Providers (e.g. for investigations)
Performance of a task carried out in the public interest	This processing is based on our need to protect recognized public interests. We may use your Personal Data to perform a task in the public interest or that is in the vital interests of an individual. See the Business Purposes of Processing section above for more information regarding the nature of processing performed for such purposes.	<u>Business Purposes</u> • Compliance, Health, Safety, Public Interest <u>Disclosures</u> • Lawful Recipients • Partners & Excursions (e.g. for health and safety)

Australia

Rights and Choices

Residents of Australia have the right under the Privacy Act to request access or correct Personal Data we hold about you, the right to erasure, and the right to withdraw any consent you may have provided with regard to processing your Personal Data. If you make a request, we will require you to verify your identity before we provide you with any access, as described in the verification requirements section.

Submission of Australian Data Requests

- **Access, Deletion or Correction:** please visit our Data Request PortalL (applicable to the specific Xanterra entity listed on the portal page).
- **Withdraw Consent (including Restriction or Do Not Sell):** please visit our Privacy Choices Portal (applicable to the specific Xanterra entity listed on the portal page).
- **For other questions or requests, please** Contact us via email to our privacy team at datarequests@xanterra.com.

Commented [HD15]: Link

Commented [HD16]: Link

Purposes of Processing

In certain cases, we may not automatically process your Personal Data for certain purposes. We rely on your consent to process Personal Data as follows:

Contexts

- Cookies and Other Tracking Technologies for Targeted Advertising
- Any context where we process certain categories of Sensitive Personal Data (including Health Data, Government ID Data, Payment Data and Precise Location Data)
- Marketing Communications

Purposes

- Targeted Advertising
- Data “Sales

Disclosures

- Advertisers, and Social Media Platforms

Regulatory Contact

You may contact the Office of the Australian Information Commissioner (OAIC) or you may contact us with any complaints regarding our privacy practices. We will respond to complaints we receive in a timely manner and process your data in accordance with your rights and our legal obligations.

Effective Date

This Privacy Policy is effective March 19, 2024.