Xanterra HR Privacy Notice
Revised Oct. 9, 2023
Download | Accessible Version

INTRODUCTION

Xanterra Leisure Holding, LLC, on behalf of itself, it subsidiaries and affiliates (collectively, "Xanterra", "we", or "us") is providing this Xanterra HR Privacy Notice ("HR Privacy Notice") to give its employees, job applicants, contractors, seafarers (collectively "Personnel") and other individuals whose Personal Data is collected for human resources purposes (such as qualified dependents) information regarding how we collect and use your Personal Data for these purposes. In this Notice, "Personal Data" (also referred to as "Personal Information" or "PI") means data relating to identified or identifiable individuals and households, and "HR Personal Data" is Personal Data collected for human resources purposes.

SCOPE OF THIS POLICY

This HR Privacy Notice applies only to Personal Data collected by Xanterra during the preceding 12-months since the effective date above and used in the context of Human Resources, employment, and other internal business functions relating to our Personnel and their family members or beneficiaries, including internal computer systems, networks, and online services. Xanterra's consumer Privacy Policy ("Privacy Policy") describes how we collect, use and protect the Personal Data of consumers and users of Xanterra's products and services, and our Digital Services (as defined in the Privacy Policy). The Privacy Policy will apply to the extent Xanterra Personnel use any products or services subject to the Privacy Policy.

CATEGORIES OF PERSONAL DATA

This chart describes the categories of Personal Data that Xanterra may collect in connection with its employment and contractual work relationships. Note, all Personal Data may be used and disclosed in connection with our Business Purposes.

Category of PI and Representative Data Elements	**Context for Collecting, Processing, and Sharing the PI**
Contact Data • Honorifics and titles, preferred form of address • Mailing address	We use your Contact Data to communicate with you by mail, email, telephone or text about your employment, including sending you work schedule information,

Category of PI and Representative Data Elements	Context for Collecting, Processing, and Sharing the PI
• Email address • Telephone number • Mobile number • Social media or communications platform usernames or handles	compensation and benefits communications and other company information. Contact Data is also used to help us identify you and personalize our communications, such as by using your preferred name.
Identity Data • Full name, nicknames or previous names (such as maiden names) • Date of birth • Language • Company ID number • Company account identifiers and passwords • Benefits program identifiers • System identifiers (e.g., usernames or online credentials)	We use your Identity Data to identify you in our HR records and systems, to communicate with you (often using your Contact Data) and to facilitate our relationship with you, for internal record-keeping and reporting, including for data matching and analytics, and to track your use of company programs and assets, and for most processing purposes described in this HR Privacy Notice, including governmental reporting, employment/immigration verification, background checks, etc.
Government ID Data • Social security/national insurance number • Driver's license information • Passport information • Other government-issued identifiers as may be needed for risk management or compliance (*e.g., if you are a licensed professional, we will collect your license number)*	We use your Government ID Data to identify you and to maintain the integrity of our HR records, enable employment verification and background screening, such as reference checks, license verifications, and criminal records checks, subject to applicable law, enable us to administer payroll and benefits programs and comply with applicable laws, such as reporting compensation to government agencies as required by law, as well as for security and risk management, such as collecting driver's license data for employees who operate company automobiles, professional license verification, fraud prevention and similar purposes . We may also use Government ID data for other customer business purposes, such as collecting passport data and secure flight information for employees, seafarers and contractors who travel.
Biographical Data	We use Qualification Information to help us understand our employees, seafarers and contractors and for professional and personal development, to assess

Category of PI and Representative Data Elements	Context for Collecting, Processing, and Sharing the PI
• Resume or CV • Data from LinkedIn profiles and similar platforms • Education and degree information • Professional licenses, certifications and memberships and affiliations • Personal and professional skills and talents summaries (e.g., languages spoken, CPR certification status, community service participation), interests and hobbies • Professional goals and interests • Criminal records	suitability for job roles, and to ensure a good fit between each individual's background and relevant job functions. We also use Qualification Information to foster a creative, diverse workforce, for coaching, and to guide our decisions about internal programs and service offerings.
Transaction and Interaction Data • Dates of Employment • Re-employment eligibility • Position, Title, Reporting Information • Work history information • Time and attendance records • Leave and absence records • Salary/Payroll records • Benefit plan records • Housing records • Travel and expense records • Training plan records • Performance records and reviews • Disciplinary records	We use Transaction and Interaction Data as needed to manage the employment relationship and fulfill standard human resources functions, such as scheduling work, providing payroll and benefits and managing the workplace (e.g. employment creation, maintenance, evaluation, discipline, etc.).
Financial Data • Bank account number and details • Company-issued payment card information, including transaction records • Credit history, if a credit check is obtained (only done in limited circumstances) • Tax-related information	We use your Financial Data to facilitate compensation, (such as for direct deposits), expense reimbursement, to process financial transactions, for tax withholding purposes, and for security and fraud prevention.

Category of PI and Representative Data Elements	Context for Collecting, Processing, and Sharing the PI
Health Data • Medical information for job placement, including drug testing and fitness to work examinations, accommodation of disabilities • Medical information for leave and absence management, emergency preparedness programs • COVID-19 testing and vaccination data, exposure to COVID-19, temperature, symptoms, travel, quarantines, and isolation status • Medical information for company housing programs • Wellness program data • Information pertaining to enrollment and utilization of health and disability insurance programs • Dietary restrictions	We use your Health Data as needed to provide health and wellness programs, including health insurance programs, and for internal risk management and analytics related to our human resources functions, staffing needs, and other Business Purposes. In response to the COVID-19 pandemic, we have implemented screening procedures, vaccination requirements, and other measures to reduce the possibility of transmission to our Personnel and guests. We may need to share this data with others for public safety reasons and compliance obligations.
Device/Network Data • Device information from devices that connect to our networks • System logs, including access logs and records of access attempts • Records from access control devices, such as badge readers • Information regarding use of IT systems and Internet access, including metadata and other technically-generated data • Records from technology monitoring programs, including suspicious activity alerts • Data relating to the use of communications systems and the content of those communications	We use Device/Network Data for system operation and administration, technology and asset management, information security incident detection, assessment, and mitigation and other cybersecurity purposes. We may also use this information to evaluate compliance with company policies. For example, we may use access logs to verify attendance records. Our service providers may use this information to operate systems and services on our behalf, and in connection with service analysis, improvement, or other similar purposes related to our business and HR functions.

Category of PI and Representative Data Elements	Context for Collecting, Processing, and Sharing the PI
Audio/Visual Data • Photographs • Video images, videoconference records • CCTV recordings • Call center recordings and call monitoring records • Voicemails	We may use Audio/Visual Data for general relationship purposes, such as call recordings used for training, coaching or quality control. We use CCTV recording for premises security purposes and loss prevention. We may also use this information to evaluate compliance with company policies. For example, we may use CCTV images to verify attendance records.
Inference Data • Performance reviews • Results of tests related to interests and aptitudes	We use inferred and derived data to help tailor professional development programs and to determine suitability for advancement or other positions. We may also analyze and aggregate data for workforce planning. Certain inference data may be collected in connection with information security functions, e.g. patterns of usage and cybersecurity risk.
Compliance and Demographic data • Diversity information • Employment eligibility verification records, background screening records, and other records maintained to demonstrate compliance with applicable laws, such as payroll tax laws, ADA, FMLA, ERISA *et al.* • Occupational safety records and worker's compensation program records • Records relating to internal investigations, including compliance hotline reports • Records of privacy and security incidents involving HR records, including any security breach notifications	We use Compliance and Demographic Data for internal governance, corporate ethics programs, institutional risk management, reporting, demonstrating compliance and accountability externally, to evaluate the diversity of our staff, and as needed for litigation and defense of claims.
Special Category Data	We use Special Category Data only as strictly necessary for the purpose it is collected with your knowledge and

Category of PI and Representative Data Elements	Context for Collecting, Processing, and Sharing the PI
Personal Data that is subject to additional restrictions under the GDPR, e.g. Personal Data revealing racial or ethnic origin, religious or philosophical beliefs, trade union membership, biometric data (if processed for the purpose of identifying a person), health information, or information relating to sexual orientation.	consent if required by law (e.g. health information on a health insurance benefits application, COVID-19 testing or vaccination status for staffing or entry into locations where vaccination or a negative test is required).
Sensitive Personal Information *(may potentially include the following)* Social security, driver's license, state identification card, or passport number; account log-in and password, financial account, number; precise location data; racial or ethnic origin, religious or philosophical beliefs, or union membership; mail, email, and text message content; the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person; data concerning health	We use Sensitive Personal Information as needed to facilitate the employment relationship, determine company housing status, for compliance and legal reporting obligations.
Protected Category Data Characteristics of protected classifications under California or federal law, e.g. race, national origin, religion, gender, or sexual orientation.	We use Protected Category Data as needed to facilitate the employment relationship, for compliance and legal reporting obligations. Please note: as each element within this category of data is included within either Sensitive Personal Information, Compliance and Demographic Data, Identity Data, or Biographical Information, it is addressed as such within this HR Privacy Notice.

SOURCES OF PERSONAL DATA

We collect Personal Data from various sources, which vary depending on the context in which we process that Personal Data.

- **Data you provide us** – We will receive your Personal Data when you provide them to us, when you apply for a job, complete forms, allow us to perform a health-related test or temperature check, or otherwise direct information to us.
- **Data we collect automatically** – We may also collect information about or generated by any device you have used to access internal IT services, applications, and networks.
- **Data we receive from Service Providers** – We receive information from service providers performing services on our behalf.
- **Data we create or infer** – We (or third parties operating on our behalf) create and infer Personal Data such as Inference Data based on our observations or analysis of other Personal Data processed under this Privacy Notice, and we may correlate this data with other data we process about you. We may combine Personal Data about you that we receive from you and from third parties.

DISCLOSURE OF PERSONAL DATA

We generally process HR Personal Data internally; however, it may be shared or processed externally by third party service providers, when required by law or necessary to complete a transaction, or in other circumstances described below.

CATEGORIES OF INTERNAL RECIPIENTS

The Personal Data identified below collected from our Personnel may be disclosed to the following categories of recipients in relevant contexts.

- **Personnel of HR Departments** – All Personal Data relating to Human Resources and Recruitment.
- **Personnel of Finance Departments** – Personal Data to the extent related to company and employee, seafarer or contractor transactions.
- **Direct Supervisors –** Elements of Personal Data to the extent permitted in the jurisdiction, to the extent necessary to evaluate, establish, and maintain the employment, seafarer or contractual relationship, conduct reviews, handle compliance obligations, and similar matters.
- **Department managers searching for new employees, seafarers or contractors** – Personal data of job candidates contained in job applications to the extent allowed by relevant laws and departmental needs.
- **Senior Supervisors –** Elements of Personal Data to the extent permitted in the jurisdiction, to the extent necessary to evaluate, establish, and maintain the employment, seafarer or contractual relationship, conduct reviews, handle compliance obligations, and similar matters.
- **IT Administrators** of Xanterra and/or third parties who support the management and administration of HR processes may receive Personal Data as necessary for providing relevant IT related support services (conducting IT security measures and IT support services)**.**

- **Peers and colleagues –** Elements of Personal Data, to the extent permitted in the jurisdiction, in connection with company address books, intracompany and interpersonal communications, and other contexts relevant to the day-to-day operation of company business.

CATEGORIES OF EXTERNAL RECIPIENTS

Xanterra may provide HR Personal Data to external third parties as described below. In addition, Xanterra may occasionally request that certain Personnel provide Personal Data directly to various service providers as needed in connection with their services on behalf of Xanterra. The specific information disclosed may vary depending on context, but will be limited to the extent reasonably appropriate given the purpose of processing and the reasonable requirements of the third party and Xanterra. We generally provide information to:

- Our subsidiaries, affiliates, and parent company.
- Service providers, vendors, and similar data processors that process Personal Data on Xanterra's behalf (e.g., analytics companies, financial analysis/budgeting, trainings, benefits administration, payroll administration, background checks, etc.) or that provide other services for our Personnel or for Xanterra.
- To prospective seller or buyer of such business or assets in the event Xanterra sells or buys any business or assets.
- To future Xanterra affiliated entities, if Xanterra or substantially all of its assets are acquired by a third party, in which case Personal Data held by it about its employees, seafarers and contractors will be one of the transferred assets.
- To your employment references, in order to inform them that you have applied with Xanterra as part of our recruiting process.
- To government agencies or departments, employee or seafarer unions, or similar parties in connection with employment related matters.
- To any public authority in relation to national security or law enforcement requests, if Xanterra is required to disclose Personal Data in response to lawful requests by a public authority.
- To any other appropriate third party, if Xanterra is under a duty to disclose or share your Personal Data in order to comply with any legal obligation or to protect the rights, property, health, or safety of Xanterra, our employees, seafarers, contractors, customers, or others.

LOCATIONS OF RECIPIENTS

Xanterra and some Xanterra affiliates are located in the United States. Any Personal Data collected under this Policy will likely be processed in the United States, in addition to any other jurisdiction where such Xanterra affiliate is located.

PURPOSES FOR COLLECTING, USING, AND DISCLOSING PERSONAL DATA

Xanterra collects Personal Data about its prospective, current, and former Personnel and other individuals for various general HR and business purposes, as described below. We do not sell or share HR Personal Data with third parties in exchange for monetary consideration or for advertising purposes.

General HR Purposes

Xanterra collects Personal Data about its prospective, current, and former Personnel and other individuals as appropriate in the context of an employment or contractual work relationship (such as dependents), including for recruitment and IT/technical support services, and as needed for using internal software, networks and devices. The categories of Personal Data we process, along with representative data elements, are listed in the chart below. We generally use, disclose and retain Personal Data processed under this HR Privacy Notice for the following purposes:

Personal Data pertaining to ***prospective*** employees, seafarers, or contractors may be collected, used and shared for:	• Recruitment and staffing, including notifying you about open positions and the status of your application, evaluation of skills and job placement, • Hiring decisions, including negotiation of compensation, benefits, relocation packages, *etc.* • Determining an individual's eligibility to work or to live in company housing (including, among other factors, whether the individual has any required vaccinations). • Risk management, including background checks reference checks, and pre-employment drug screening. • Our Business Purposes (defined below).
Personal Data pertaining to ***current*** employees, seafarers, and contractors may be collected, used and shared for:	• Staffing and job placement, including scheduling and absence management, • Administration of compensation, insurance and benefits programs, • Administration of company housing programs, • Time and attendance tracking, expense reimbursemen other workplace administration and facilitating relationships within Xanterra,

	• IT uses, such as managing our computers and other assets, providing email and other tools to our workers, • EEO/Affirmative Action programs, • Health and wellness programs, • Reasonable accommodations, • Occupational health and safety programs (including drug and alcohol testing, required injury and illness reporting, disaster recovery and business continuity planning, and workers' compensation management), • Health and safety requirements imposed by Xanterra, government authorities, or others, depending on the location of employment, engagement or travel (e.g. vaccination status or health screening), • Talent and performance development, skills management and training, performance reviews, employee feedback surveys, and recognition and reward programs, • HR support services, such as responding to inquiries, providing information and assistance, and resolving disputes, • Risk management and loss prevention, including employee and premises monitoring, such as in our retail locations, or adjacent to Xanterra premises, • Implementing an effective sickness absence management system including monitoring the amount of leave and subsequent actions to be taken, such as making adjustments, • Managing statutory leave programs such as family and parental leave, • Succession planning and adjustments for restructuring • Providing employment and income verification, • As requested by individuals, and • Business Purposes.
Personal Data pertaining to ***former*** employees, seafarers, and contractors may be collected, used and shared for:	• Re-employment, • Administration of compensation, insurance and benefits programs, • For archival and recordkeeping purposes, • Providing employment and income verification, • As requested by individuals, and • Business Purposes.

Personal Data pertaining to individuals whose information is provided to Xanterra in the course of ***HR management*** (such as information pertaining to employees' family members, beneficiaries, dependents, emergency contacts, *etc.*) may be collected, used and shared for:	• Administration of compensation, insurance and benefit programs, • Administration of company housing programs, • Workplace administration, • To comply with child support orders or garnishments, • To maintain internal directories, emergency contact lists and similar records, and • Business Purposes.

Business Purposes

"Business Purposes" means the following purposes for which Personal Data may be collected, used and shared:

- Maintaining comprehensive and up-to-date Personnel records,
- Identity and credential management, including identity verification and authentication, issuing ID card and badges, system administration and management of access credentials,
- Security, loss prevention, information security and cybersecurity,
- Legal and regulatory compliance, including without limitation all uses and disclosures of Personal Data that are required by law or for compliance with legally mandated policies and procedures, such as anti-money laundering programs, security and incident response programs, intellectual property protection programs, and corporate ethics and compliance hotlines, and other processing in connection with the establishment and defense of legal claims,
- Corporate audit, analysis and consolidated reporting,
- To enforce our contracts and to protect Xanterra, our workers, our clients and their employees and the public against injury, theft, legal liability, fraud or abuse, to people or property,
- As needed to de-identify the data or create aggregated datasets, such as for consolidating reporting, research or analytics,
- Making back-up copies for business continuity and disaster recovery purposes, and other IT support, debugging, security, and operations,
- For the analysis and improvement of technical and organizational services, operations, and similar matters;
- To communicate with you regarding your position, benefits, and other HR matters; and
- As needed to facilitate corporate governance, including mergers, acquisitions and divestitures.

DATA ADMINISTRATION

SECURITY

Xanterra requires that Personal Data be protected using technical, administrative, and physical safeguards, as described in our various security policies. Xanterra staff must follow the security procedures set out in applicable security policies at all times.

COMMUNICATION PREFERRENCES

Update Communication Preferences

You may update your communication preferences with Xanterra at any time. If you are a prospective employee, navigate to the external job board (apply-xanterra.icims.com). Select "Log back in!" at the top. From there, your dashboard appears. Select "Profile & Resume." Edit the phone number or email address listed on your profile. Then select "Update Profile" at the bottom to save those changes.

If you are a current or returning employee, navigate to the internal job portal (internal-xanterra.icims.com). Then select "Log back in!" at the top. From there your dashboard appears. Select "Profile & Resume." Edit the phone number or email address listed on your profile. Then select "Update Profile" at the bottom to save those changes.

Opt-Out of Text Communications

If you prefer to no longer receive text communications from Xanterra, please reply STOP to quit. Msg&Data rates may apply.

Opt-Out of Email Communications

If you do not wish to receive emails in the future about job opportunities, please navigate to (https://www.xanterrajobs.com/talent-network/talentcommunity). Then select "Already a member? Click here" to log in. Your dashboard will open and you can select "Emails & Alerts." Uncheck the box for "I would like to receive email communication for marketing and/or general engagement purposes."

RETENTION AND DISPOSAL

Xanterra keeps Personal Data only for the amount of time reasonably needed to fulfill the legitimate business purpose for which it was collected or to satisfy a legal requirement. 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 Personal 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 with continued processing, retention, and deletion.

We will review retention periods periodically and may pseudonymize or anonymize data held for longer periods. Xanterra staff must follow any applicable records retention schedules and policies and destroy any media containing Personal Data in accordance with applicable company policies.

A partial list of Personal Data we maintain for HR business purposes, and the retention period, is below.

Category of Personal Data	**Retention Period OR Criteria Used to Determine Retention Period**
Background Check Reports	5-7 years depending on whether on an applicant or employee
Employee Benefits Records	Life of benefits + 6 years (some exceptions)
COBRA, Family and Medical Leave Act	Year employment is terminated + 7 years
Drug Testing	Year employment is terminated + 7 years (note: mandated testing for Dept. of Transportation is 5 years after expired/superseded, and mandated but negative is 2 years)
EEOC Filings & AA Plan Records	Expired or superseded + 7 years
Payroll	8 Years
Immigration Records	Year employment is terminated + 7 years
Employment Records – Hired Personnel	Year employment is terminated + 7 years
Employment Records – Unhired Personnel	2 years (4 years in CA)
OSHA Records	Year employment is terminated + 40 years for toxic and bloodborne pathogen records All other: Year employment is terminated + 7 years
OSHA Form 300	5 years following the end of the year to which they relate
Payroll Registers, Time & Attendance	Year employment is terminated + 8 years
Personnel Records (ADEA, Title VII/ADA, and other Discrimination Issues)	Year employment is terminated + 7 years

Investigations	Completion + 5 years
Motor Carrier Driver Qualifications	Employment Termination + 3 years
Driver Service Hours	6 Months
Salary Administration	8 Years
Employee Non-Exposure Medical Records	Employment Termination + 6 years
Employee Relocation Records	5 years
General	Year employment is terminated + 7 years

YOUR CALIFORNIA PRIVACY RIGHTS

Under the California Consumer Privacy Act ("**CCPA**") and other comprehensive state privacy laws, residents of California may have the following rights, subject to your submission of an appropriately verified request (see below for verification requirements):

Right to Know

You may request any of following, for the 12 month period preceding your request: (1) the categories of Personal Data we have collected about you, or disclosed for a commercial purpose; (2) the categories of sources from which your Personal Data was collected; (3) the business or commercial purpose for which we collected, sold or shared your Personal Data; (4) the categories of third parties to whom we have sold or shared your Personal Data, or disclosed it for a business purpose; and (5) the specific pieces of Personal Data we have collected about you.

Right to Delete	You have the right to delete certain Personal Data that we hold about you, subject to exceptions under applicable law.
Right to Correct	You have the right to correct certain Personal Data that we hold about you, subject to exceptions under applicable law.
Right of Non-retaliation	You have the right to not to receive discriminatory treatment as a result of your exercise of rights conferred by the CCPA.
Direct Marketing	You may request a list of Personal Data we have disclosed about you to third parties for direct marketing purposes during the preceding calendar year, if applicable.
Minors'	To the extent we have actual knowledge that we collect or maintain Personal Data of a minor under age 16, those minors between the age of 13 and 16 must opt in to any sharing of personal information (as defined under CCPA), and minors under the age of 13 must have a parent consent to sharing of personal information (as defined under CCPA). All minors have the right to opt-out later at any time. Minors under age 13 may have other rights under the Children's Online Privacy Protection Act ("COPPA").

Verification of Requests

Requests to receive a copy of Personal Data, and requests to delete or correct Personal Data, must be verified to ensure that the individual making the request is authorized to make that request, to reduce fraud, and to ensure the security of your Personal Data. We may require that you log in through Xanterra Go (if you are a current employee, and/or that you provide the email address we have on file for you (and verify that you can access that email account) as well as an address, phone number, or other data we have on file, in order to verify your identity. 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.

ADDITIONAL DISCLOSURES – UK/EU/EEA/INTERNATIONAL RESIDENTS

GDPR PRIVACY RIGHTS

Under the General Data Protection Regulation ("GDPR") and analogous legislation, residents of the UK, EU/EEA, Switzerland, Cayman Islands, and other locations may have the following rights in addition to those set forth in the Rights & Choices section above, subject to applicable legal limitations, and provided that your request is appropriately verified:

- **Access** – You may have a right to know what information we collect, use, disclose, or sell, and you may have the right to receive a list of that Personal Data and a list of the third parties (or categories of third parties) with whom we have received or shared

Personal Data, to the extent required and permitted by law. You may be able to access some of the Personal Data we hold about you directly through the Xanterra employee portal.

- **Rectification** – You may correct any inaccuracies in Personal Data that we hold about you to the extent required and permitted by law. You may be able to make changes to much of the information you provided to us using the Xanterra employee portal.
- **Delete** – To the extent required by applicable law, you may request that we delete your Personal Data from our systems. We may delete your data entirely, or we may anonymize or aggregate your information such that it no longer reasonably identifies you. Contact us as part of your request to determine how your Personal Data will be erased in connection with your request.
- **Data Export** – To the extent required by applicable law, we will send you a copy of your Personal Data in a common portable format of our choice.
- **Objection** – You may have the right under applicable law to object to (or to restrict) our processing of your Personal Data that we undertake without your consent, as in connection with our legitimate business interests (including any processing specified as such, or processed under this Privacy Policy for a Business Purpose). You may do so by contacting us re: data rights requests. Note that we may not be required to cease, or limit processing based solely on that objection, and we may continue processing cases where our interests in processing are balanced against individuals' privacy interests. You may also object to processing for direct marketing purposes. We will cease processing upon your objection to such processing.
- **Automated Decision-Making** – You may have the right to regulate any automated decision-making or profiling of Personal Data if it adversely affects your legal rights.
- **Regulator Contact** – You may have the right to contact or file a complaint with regulators or supervisory authorities about our processing of Personal Data. To do so, please contact your local data protection or consumer protection authority.

LEGAL BASIS FOR PROCESSING PERSONAL DATA

We process Personal Data in connection with the management and administration of HR processes as described below. For example, we process Personal Data when we have a legitimate interest in the processing of that data, such as:

- To **improve recruitment processes** and staffing, e.g., by monitoring characteristics and qualifications of applicants.
- To provide **training and professional development** services to Personnel.
- To track, manage and **process Personnel expenses**, and other company finances submitted by or related to Personnel.

- To monitor **compliance with our IT and data security/use policies**, for example, to ensure that confidential information is not sent outside the network, or to ensure the proper use of employer-provided technologies (including communications). Note: such processing may include access by Xanterra to the content of communications sent using Xanterra equipment or services.
- To **manage Personnel and improve internal processes and systems**, for example, to monitor attendance and productivity, and create records of Personnel certifications, disciplinary history, and other records not required by law.
- To provide **communications services to** Personnel, as well as providing **on-site and remote networking** such as VPNs, Wi-Fi, and related logins, and when we monitor the operation and security of those services.
- To **provide and manage hardware, and software applications** that are used in business operations, e.g. when a user is assigned a given device (e.g. a laptop or computer), or user account (e.g. for software or SaaS services).
- To **support Personnel's use of essential or important technology services**, e.g. when we provide technical support.
- For **physical and information security** purposes, we may process Personal Data when we monitor and filter network traffic, scan communications for malware, and use video monitoring in our facilities.

We may also process Personal Data whenever it is strictly necessary in connection with certain activity, such as**:**

- To **maintain a relationship or fulfil a contract** – for example, processing Personal Data to pay our Personnel or reimburse expenses, as part of essential employment records, and any processing of Personal Data that you may provide in connection with benefits (such as insurance or retirement accounts).
- To **comply with Xanterra's legal obligations** – for example, processing immunization status and other health-related Personal Data in order to provide a safer working environment for our Personnel and our guests, sharing Personal Data with regulatory agencies in connection with tax and income reporting, and providing Personal Data in response to legal requests or for regulatory or law enforcement purposes.
- To **protect vital interests of individuals** – for example, using Personal Data to contact individuals in an emergency, to provide information in connection with health and safety incidents, or in order to ensure the health, safety and welfare of our Personnel and guests.

We process **Special Category information** only when permitted by law. For example:

- When in the **public interest or required by law**, e.g. in connection with legal and regulatory reporting requirements relating to taxation, public health, etc., including as needed to ensure all Personnel and guests (in some locations) have received COVID-19 vaccinations or have passed other applicable health screening measures.

- To protect an individual's **vital interests** when consent cannot be obtained, e.g. in a workplace injury.
- In connection with our **rights and obligations under law**, e.g. in connection with legal reporting requirements.
- As may be necessary **for the defense of legal claims**, e.g. potential claims that we have not provided a safe environment, or claims that may arise from charges of not complying with legal requirements.

Finally, we may process any Personal Data in accordance with **your consent**, for example, in connection with your participation in an optional program, event, or other endeavor. You also have the right to withdraw that consent at any time. However, in some cases, we may continue to process the Personal Data where we have another legal basis for doing so, such as described above.

INTERNATIONAL TRANSFERS

In most instances, Xanterra is a US-based employer. To the extent the Personal Data is subject to GDPR, it will be necessary for us transfer Personal Data to, and process it in, the United States in order to evaluate, establish, and maintain the employment relationship, and your Personal Data will be transferred to the US on that basis.

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 cooperate and comply respectively with the advice of the panel established by the EU data protection authorities (DPAs), the UK Information Commissioner's Office (ICO) and the Gibraltar Regulatory Authority (GRA), and the Swiss Federal Data Protection and Information Commissioner (FDPIC), with regard to unresolved complaints concerning our handling of human resources 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 in the context of the employment relationship.

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/framework-article/ANNEX-I-introduction.

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.

HOW TO CONTACT US

Please submit your data rights requests through our HR Data Rights portal or call 844-388-2813. For all other questions or comments about this HR Privacy Notice or our privacy practices, please contact our Data Privacy Team under General Inquiries:

Xanterra Leisure Holding, LLC
Attn: Privacy
6312 S. Fiddlers Green Cir. Ste. 600N
Greenwood Village, CO 80111
All Personnel Inquiries: CorpHR@Xanterra.com.