PRIVACY POLICY FOR MOTOR CARRIERS

Policy Statement

Union Pacific Railroad Company ("UP" or the "Company") collects and retains certain information from you, including your finger scan, to increase security and control access to certain facilities and properties of UP. Your finger scan may be considered a biometric under various state laws. UP recognizes the sensitivity of Personal Information and Biometric Information and takes seriously its obligations to maintain the confidentiality and protect the security of the data. In accordance with state and federal laws and regulations, this policy sets forth the Company's procedures for disclosure, storage and destruction of Personal Information and Biometric Information.

Definitions

Personal Information. Information that identifies, relates to, describes, references, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual, consumer or device.

Biometric Identifier. A finger scan, voiceprint, retina or iris scan, hand or face geometry scan, and analysis based on these identifiers.

Biometric Information or Biometric Data. An individual's physiological, biological or behavioral characteristics, including an individual's deoxyribonucleic acid (DNA), that can be used, singly or in combination with each other or with other identifying data, to establish individual identity. Biometric information includes, but is not limited to, imagery of the iris, retina, finger scan, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.

Information We Collect

We may have collected the following categories of Personal Information from you within the last twelve (12) months:

Category	Examples	Collected
A. Identifiers	A real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, Social Security number, driver's license number, passport number, or other similar identifiers	Yes
B. Personal information categories listed in the California Customer	A name, signature, Social Security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification	Yes

Records statute (Cal. Civ. Code § 1798.80(e))	card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information. Some personal information included in this category may overlap with other categories	
C. Protected classification characteristics under California or federal law	Age (40 years or older), race, color, ancestry, national origin, citizenship, religion or creed, marital status, medical condition, physical or mental disability, sex (including gender, gender identity, gender expression, pregnancy or childbirth and related medical conditions), sexual orientation, veteran or military status, genetic information (including familial genetic information)	No
D. Commercial information	Records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.	No
E. Biometric information	Genetic, physiological, behavioral, and biological characteristics, or activity patterns used to extract a template or other identifier or identifying information, such as, finger scans, faceprints, and voiceprints, iris or retina scans, keystroke, gait, or other physical patterns, and sleep, health, or exercise data	Yes
F. Internet or other similar network activity	Browsing history, search history, information on a consumer's interaction with a website, application, or advertisement	No
G. Geolocation data	Physical location or movements	No
H. Sensory data	Audio, electronic, visual, thermal, olfactory, or similar information	No
I. Professional or employment-related information	Current or past job history or performance evaluations	Yes
J. Non-public education information (per the Family Educational Rights and Privacy Act (20 U.S.C. Section 1232g, 34 C.F.R. Part 99))	Education records directly related to a student maintained by an educational institution or party acting on its behalf, such as grades, transcripts, class lists, student schedules, student identification codes, student financial information, or student disciplinary records	No
K. Inferences drawn from other personal information	Profile reflecting a person's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes	No

We obtain the categories of Personal Information listed above from the following categories of sources:

- Directly from you or your employer. For example, from documents that your employer provided to us related to the services they provide.
- Directly and indirectly from activity related to the services you provide. For example, when you use your finger scan to access our facilities and property.

Use of Personal Information

We may use or disclose the Personal Information we collect for one or more of the following business purposes:

- To carry out our obligations and enforce our rights arising from any contracts entered into between your employer and us.
- As necessary or appropriate to protect the rights, property or safety of us, our clients or others.
- To respond to law enforcement requests and as required by applicable law, court order, or governmental regulations.
- As described to you when collecting your Personal Information or as otherwise set forth in the California Consumer Protection Act (CCPA).
- To evaluate or conduct a merger, divestiture, restructuring, reorganization, dissolution, or other sale or transfer of some or all of our assets, whether as a going concern or as part of bankruptcy, liquidation, or similar proceeding, in which Personal Information held by us is among the assets transferred.

We will not collect additional categories of personal information or use the Personal Information we collected for materially different, unrelated, or incompatible purposes without providing you notice.

Sharing Personal Information

We may disclose your Personal Information to a third party for a business purpose. When we disclose Personal Information for a business purpose, we enter a contract that describes the purpose and requires the recipient to both keep that Personal Information confidential and not use it for any purpose except performing the contract.

We disclose your Personal Information for a business purpose to the following categories of third parties:

- Our affiliates.
- Service providers.

- Third parties to whom you or your employer authorize us to disclose your Personal Information.
- As required by state or federal law or municipal ordinance.
- As required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.
- To persons or entities where you have consented to such disclosure or dissemination.

We have not and will not sell any Personal Information.

California Residents - Your Rights and Choices

The CCPA provides California residents with specific rights regarding their Personal Information. This section describes California residents' CCPA rights and explains how to exercise those rights.

Access to Specific Information and Data Portability Rights

You have the right to request that we disclose certain information to you about our collection and use of your Personal Information over the past 12 months. Once we receive and confirm your verifiable consumer request, we will disclose to you:

- The categories of Personal Information we collected about you.
- The categories of sources for the Personal Information we collected about you.
- Our business or commercial purpose for collecting or using that Personal Information.
- The categories of third parties with whom we share that Personal Information.
- The specific pieces of Personal Information we collected about you (also called a data portability request).
- If we disclosed your Personal Information for a business purpose.

Deletion Request Rights

You have the right to request that we delete any of your Personal Information that we collected from you and retained, subject to certain exceptions. Once we receive and confirm your verifiable request, we will delete (and direct our service providers to delete) your Personal Information from our records, unless an exception applies.

We may deny your deletion request if retaining the information is necessary for us or our service providers to:

1. Complete the transaction for which we collected the Personal Information, take actions reasonably anticipated within the context of our ongoing business relationship with your employer, or otherwise perform our contract with your employer.

2. Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for such activities.
3. Comply with a legal obligation.
4. Make other internal and lawful uses of that information that are compatible with the context in which you provided it.
5. Enable solely internal uses that are reasonably aligned with consumer expectations based on your relationship with us.

Exercising Access, Data Portability, and Deletion Rights

To exercise the access, data portability, and deletion rights described above, please submit a verifiable request to us by either:

- Calling us at 1-866-251-9185, or
- Visiting CCPA-Request@up.com.

Only you or a person registered with the California Secretary of State that you authorize to act on your behalf may make a verifiable request related to your Personal Information.

You may only make a verifiable consumer request for access or data portability twice within a 12-month period. The verifiable consumer request must:

- Provide sufficient information that allows us to reasonably verify you are the person about whom we collected Personal Information or an authorized representative.
- Describe your request with sufficient detail that allows us to properly understand, evaluate, and respond to it.

We cannot respond to your request or provide you with Personal Information if we cannot verify your identity or authority to make the request and confirm the Personal Information relates to you. We will only use Personal Information provided in a verifiable request to verify the requestor's identity or authority to make the request.

Response Timing and Format

We endeavor to respond to a verifiable consumer request within 45 days of receipt. If we require more time (up to 90 days), we will inform you of the reason and extension period in writing. We will deliver our written response by mail or electronically, at your option. Any disclosures we provide will only cover the 12-month period preceding the verifiable request's receipt. The response we provide will also explain the reasons we cannot comply with a request, if applicable. For data portability requests, we will select a format to provide your Personal Information that is readily useable and should allow you to transmit the information from one entity to another entity without hindrance.

We do not charge a fee to process or respond to your verifiable request unless it is excessive, repetitive, or manifestly unfounded. If we determine that the request warrants a fee, we will tell you why we made that decision and provide you with a cost estimate before completing your request.

Non-Discrimination

We will not discriminate against you for exercising any of your CCPA rights.

Changes to Our Privacy Notice

We reserve the right to amend this privacy notice at our discretion and at any time. When we make changes to this privacy notice, we will notify you by email or through a notice on our website homepage.

Policy Implementation

Consent. An individual's Biometric Data will not be retained, collected or otherwise obtained by UP without prior written consent of the individual. The consent form will inform the individual of the reason the Biometric Information is being collected and the length of time the data will be stored.

Storage. In circumstances where UP retains Personal Information, UP will use a reasonable standard of care to store, transmit and protect from disclosure any paper or electronic Personal Information collected. Storage, transmission, and protection from disclosure shall be performed in a manner that is the same as or more protective than the manner in which the Company stores, transmits and protects from disclosure other confidential and sensitive information that is used to uniquely identify an individual.

Retention Schedule. Unless subject to a legal hold or other specific legal requirement, UP will permanently destroy an individual's Personal Information within three (3) years of when the initial purpose for collecting or obtaining such Personal Information has been satisfied, such as (a) the individual no longer is permitted access to UP property and facilities; or (b) UP no longer uses the Personal Information.

Contact Information

The following office can address questions regarding this Policy: 1-866-251-9185; email: CCPA-Request@up.com.

Updated: February 2020