

# CCPA - First Transit Privacy Policy and Notice for California Residents

## Introduction

## Information we collect about California consumers

## Sources of personal information (CA)

## Use of personal information (CA)

## Disclosure and sharing of personal information

## Disclosure of personal information for business purposes

## Cookies/Tracking Technologies

## Other sharing

## Your California rights and choices

## Personal information sales opt-out and opt-in rights

## Non-Discrimination

## Other California privacy rights

## Contact us

# Privacy Policy and Notice for California Consumers

## Introduction

**Effective Date:** January 1, 2022

**Last updated on:** December 20, 2021

This Privacy Policy and Notice for California consumers supplements the information contained in FirstGroup's [Privacy Policy](#) and applies solely to California residents ("**consumers**" or "**you**"). We adopt this notice to comply with the California Consumer Privacy Act of 2018 (including its later amendments and implementing regulations) ("**CCPA**") and any terms defined in the CCPA have the same meaning when used in this notice.

As with our Privacy Policy, "FirstGroup" means FirstGroup America, Inc., First Transit, Inc., First Student, Inc., First Canada ULC, First Transit Canada ULC, and their affiliated companies.

This notice does not apply to workforce-related personal information we collect from our California-based employees, job applicants, contractors, or similar individuals, for whom we have separate CCPA collection notices.

Where noted in this notice, the CCPA temporarily exempts personal information reflecting a written or verbal business-to-business communication ("**B2B information**") from some of its requirements.

## Information we collect about California consumers

We collect information that identifies, relates to, describes, references, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer, household, or device ("**personal information**").

Personal information does not include:

- Publicly available information from government records.
- Deidentified or aggregated consumer information.
- Information excluded from the CCPA's scope, like:
  1. Health or medical information covered by the Health Insurance

Portability and Accountability Act of 1996 (HIPAA) and the California Confidentiality of Medical Information Act (CMIA), clinical trial data, or other qualifying research data;

2. Personal information covered by certain sector-specific privacy laws, including the Fair Credit Reporting Act (FCRA), the Gramm-Leach-Bliley Act (GLBA) or California Financial Information Privacy Act (FIPA), and the Driver's Privacy Protection Act of 1994.

The information we collect and have collected about California consumers in the last 12 months corresponds with the categories of personal information under the CCPA in the table below. When any of the information we collect meets the definition of "personal information" under the CCPA we will treat it in accordance with the CCPA's requirements.

Category	Examples	Do we collect this information?
A. Identifiers	This may include, but is not limited to, your name, alias, mailing address, home address, work address, unique personal identifiers, online identifiers, IP addresses, email addresses, account name, Social Security number, or other similar identifiers.	YES

<p>B. Personal information categories listed in the California Customer Records statute (Cal. Civ. Code § 1798.80(e))</p>	<p>This may include information such as your name, signature, Social Security number, address, telephone number, credit or debit card number, bank account number, or other financial information, education or employment-related information, medical information, or health insurance information.</p> <p>Some personal information included in this category may overlap with other categories.</p>	<p>YES</p>
<p>C. Protected classification characteristics under California or federal law</p>	<p>In connection with some of our services, we may collect information that has been designated a protected classification characteristic under California or federal law. This may include, but is not limited to, age (40 years or older), medical condition, physical or mental disability, veteran, or military status).</p>	<p>YES</p>
<p>D. Commercial information</p>	<p>This may include information such as records of services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.</p>	<p>YES</p>

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, fingerprints, faceprints, and voiceprints, iris or retina scans, keystroke, gait, or other physical patterns, and sleep, health, or exercise data.	NO
F. Internet or other similar network activity	This may include such information as your browsing history, search history, information on a consumer's interaction with a website, application, or advertisement.	YES
G. Geolocation data	In some cases, we may collect geolocation data to provide location-related services to our customers and riders.	YES
H. Sensory data	We may collect audio information if you call our offices and leave a voicemail or if your call with one of our customer service representatives is recorded for quality assurance or training purposes. We collect visual information through our use of CCTV.	YES

I. Professional or employment-related information	We may collect professional or employment-related information about you. For example, we may collect information related to your place of employment and travel history to and from work.	YES
J. Non-public education information (per the Family Education Rights Privacy Act, 20 U.S.C. Section 1232g, 34 C.F.R. Part 99)	When we provide transportation services to our customers who hire us to transport students, we may collect non-public education records directly related to a student maintained by an education institution or party acting on its behalf, such as class lists, student IDs, student behavioral and disciplinary records, a student's grade, schedule-related information, and disability information including information contained in Individual Education Plans (IEPs) and Section 504 plans.	YES
K. Inferences drawn from other personal information	Profile reflecting a person's preferences, including brand or product preferences and purchasing preferences.	YES

## Sources of personal information

We obtain the categories of personal information listed above from the following categories of sources:

### When you provide it

We collect information when you provide it

through your direct interactions with us including, for example, when you:

- Fill in forms or contact us through our website, via telephone, or email.
- Create an online account or access our services through your online account.
- Use our websites or apps to search transportation routes and schedules, on-demand transportation, or other transportation options.
- Buy transit tickets, charter a bus, or purchase or use one of our other services.
- Report a problem with one of our websites, apps, or give us feedback on our services.

### **Automatically from our websites, apps, and emails**

As you interact with our websites, apps, or emails, we automatically collect technical information and usage information about your equipment, browsing actions and patterns. We collect this information by using cookies, server logs, web beacons, and other similar technologies.

### **From others**

We may also receive personal information about you from third parties such as:

- Our service providers when we request that they collect information on our behalf.
- Our riders (and other users of our services) including, for example, riders who provide us information about family members or other persons.
- Our customers who have outsourced the provision of specific services to us. Our customers include government and quasi government entities, political subdivisions, and public authorities (including, for example, transit authorities and airports); public school districts; institutions of higher learning; for-profit businesses; and non-profit organizations.
- Other companies or organizations that provide us with data in accordance with applicable law. These companies or organizations may include ad tech companies, data analytic providers, government entities, and online platforms including social media networks.

### **From closed-circuit television (CCTV)**

We use CCTV cameras to capture, record and monitor what takes place at our facilities and on some of our buses and other transit vehicles to help us provide a safe environment for our passengers, employees, and the general public and to prevent, deter and detect crime.

## **Use of personal information**

We may use, disclose, or share the personal information for one or more of the following purposes:

- to provide, support, personalize, develop, troubleshoot, and improve websites and apps, and to notify you about changes to the same.
- to improve our services and communicate with you. In some cases, we may record our telephone calls with you for quality assurance purposes.
- to provide accommodations to disabled persons.
- in cases where we offer this option to our customers, to create, maintain, and secure an online account with us.
- to determine your eligibility for (and report your use of) our services according to our contracts with customers, applicable laws and our policies.
- to process your requests, transactions, and payments and to provide transportation services.
- to process and issue refunds.
- provide customer service and send transactional messages.
- to recommend transportation routes, mobility service options, and other services that you request.
- to send marketing communications, surveys, or invitations.
- to interact with you on social media.
- to maintain the safety, security, and integrity of our websites, apps, databases, and other technology assets.
- to investigate and prevent fraud and other criminal activity.
- to manage and improve our marketing or customer relationships and experiences. For example, we may use your information to optimize station use, improve operational efficiency, and to increase ridership.
- to protect the health, safety and general well-being of riders, employees, customers, and general public, which may in some cases include collection by way of a video camera placed in a bus or other vehicle.
- to administer the physical security of the FirstGroup facilities including transit stations, which may in some cases include collection by way of a video surveillance system.
- to receive, investigate and address inquiries or complaints from riders, customers, and others.
- to process or settle insurance claims.
- to conduct credit checks, as well as to administer the billing and payment process.
- to measure or understand the effectiveness of the advertising we serve to you and others, and to deliver more relevant content and advertising.
- to investigate and respond to legal matters.

- to carry out our obligations and enforce our rights arising from any contracts with you, including for billing and collection or to comply with legal requirements.
- 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 is among the assets to be transferred.
- in any other way we may describe when you provide the information or to fulfill the purpose for which you provided it (this may include purposes that are not materially different, unrelated, or incompatible with the purpose described).

## Disclosure and sharing of personal information

The business and commercial purposes that we may disclose or share your personal information are described above and in our [Privacy Policy](#). More specific information on that sharing follows:

### Disclosure of personal information for business purposes

We may disclose your personal information for a business purpose pursuant to a written contract that limits the recipient's ability to use and disclose the personal information for purposes other than performing the contract. FirstGroup discloses (and has disclosed within the previous 12 months) personal information for a business purpose to the categories of recipients indicated below.

Personal Information Category	Categories of Recipients
A: Identifiers.	Service providers, banks, data analytics providers, external agencies, external auditors, customers.
B: California Customer Records personal information categories.	Service providers, banks, external agencies, external auditors, customers
C: Protected classification characteristics under California or federal law.	Service providers, external agencies, external auditors, customers
D: Commercial information.	Service providers, banks, external agencies, external auditors, customers
E: Biometric information.	None. We do not collect biometric information.



F: Internet or other similar network activity.	Service providers and external auditors, data analytics providers
G: Geolocation data.	Service providers, external agencies, external auditors, customers
H: Sensory data.	Service providers, external agencies, external auditors, customers
I: Professional or employment-related information.	Service providers, external agencies, external auditors, customers
J: Non-public education information.	Service providers, customers
K: Inferences drawn from other personal information.	Service providers, customers

### Cookies/Tracking Technologies

Some of our websites use cookies or other tracking technologies in a manner that is likely considered to be a “sale” under the CCPA. In the context of cookies or other similar technologies, we have shared the following categories of personal information during the last 12 months:

<b>Personal Information Category</b>	<b>Categories of Recipients</b>
A: Identifiers.	Online platforms, ad tech companies
B: California Customer Records personal information categories.	None
C: Protected classification characteristics under California or federal law.	None
D: Commercial information.	Online platforms, ad tech companies
E: Biometric information.	None
F: Internet or other similar network activity.	Online platforms, ad tech companies
G: Geolocation data.	Online platforms, ad tech companies
H: Sensory data.	None
I: Professional or employment-related information.	None
J: Non-public education information.	None
K: Inferences drawn from other personal information.	Online platforms, ad tech companies

We do not sell personal information of consumers we know are younger than 16 years old or information that we are prohibited from selling under applicable law.

## Other sharing

Apart from “sales” that may occur because of the cookies and tracking technologies that we use on some of our websites, we do not sell personal information. However, we offer a “DO NOT SELL” opt-out for non-cookie type of “sales” in case we later change our business practices.

We never sell the following:

- personal information of consumers we know are younger than 16 years old.
- personal information that we are prohibited from selling under applicable law.
- personal information we collect or process on behalf of our B2B customers when we act as a “service provider,” as that term is defined in the CCPA.

For more information about your personal information sale rights, see the section below titled “Personal Information sales opt-out and opt-in rights.”

## Your California rights and choices

The CCPA provides consumers (California residents) with specific rights regarding their personal information.

In many cases we act as a service provider to our customers. In such cases, you will need to exercise your rights directly with our customer. If you make a request with respect to personal information that we have collected or otherwise maintain in our role as a service provider, then, unless we have agreed to respond to and fulfill CCPA requests on our customer's behalf, we will let you know that we cannot fulfill the request.

This section describes your CCPA rights and explains how to exercise those rights in cases where we collect, maintain, or share data outside of our role as a service provider.

### Your right to know

You have the right to request that we disclose certain information to you about our collection, use, disclosure, and sale of your personal information (the “right to know”). Once we receive your request and verify your identity (as described below), 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.
- The business or commercial purpose for collecting or selling that personal information.
- The categories of third parties with whom we share that personal information.
- If we sold or disclosed your personal information for a business purpose, two separate lists disclosing:

- sales, identifying the personal information categories that each category of recipient purchased; and
- disclosures for a business purpose, identifying the personal information categories that each category of recipient obtained.

We do not provide right to know rights to B2B information.

### **Your right to get a copy**

You have a right to obtain a copy of the specific pieces of personal information we collected about you (also called a data portability request). Once we receive your request and verify your identity (as described below), we will provide you a copy of your personal information that is responsive to your request.

We do not provide portability rights to B2B information.

### **Your right to delete**

You have the right to request that we delete personal information that we have collected from you and retained, subject to certain exceptions. Once we receive your request and verify your identity, we will review the request to see if an exception applies that allows us to retain some or all your information. 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, provide a good or service that you requested, take actions reasonably anticipated within the context of our ongoing business relationship with you, fulfill the terms of a written warranty or product recall conducted in accordance with federal law, or otherwise perform our contract with you.
2. Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for such activities.
3. Debug products to identify and repair errors that impair existing intended functionality.
4. Exercise free speech or to ensure the right of another consumer to exercise their free speech rights, or exercise another right provided for by law.
5. Comply with the California Electronic Communications Privacy Act (Cal. Penal Code § 1546 et. seq.).
6. Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the information's deletion may likely render impossible or seriously impair the research's achievement, if you previously provided informed consent.
7. Enable solely internal uses that are reasonably aligned with consumer expectations based on your relationship with us.
8. Comply with a legal obligation.

9. Make other internal and lawful uses of that information that are compatible with the context in which you provided it.

We will delete or deidentify personal information not subject to one of these exceptions from our records and will direct our service providers to take similar action. If an exception applies, we will provide you information about that exception.

We do not fulfill deletion requests for B2B information.

### **Exercising your rights to know, delete or obtain a copy of your personal information**

To exercise your right to know, your right to obtain a copy of your information, or your right to delete as described above, please submit a request by either:

- Completing this [FORM](#) on our CCPA request portal.
- Calling us at 1-844-930-1776.

If you are disabled and need reasonable accommodations to facilitate your request, please let us know.

We will only use personal information provided in a consumer request to verify the requestor's identity or authority to make the request and to locate relevant information. 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 cannot delete personal information in those situations where our retention is required for our own internal business purposes or otherwise permitted by the CCPA (such as fraud prevention or legal compliance). In these situations, we will retain your information in accordance with our records retention program and securely delete it at the end of the retention period.

Information on how to exercise your sale opt-out or opt-in rights can be found below.

### **Who may submit requests?**

Only you, or someone legally authorized to act on your behalf (an authorized agent), may make a request to know, obtain a copy, or delete your personal information.

If you use an authorized agent to submit a request to know or a request to delete, we may require that the authorized agent provide us with proof that you gave the agent signed permission to submit the request. If an authorized agent does not have power of attorney pursuant to the California Probate Code, then we may also require you to do either of the following: (1) verify your own identity directly with us; or (2) directly confirm with us that you have provided the authorized agent permission to submit the request on your behalf. Finally, if your authorized agent is a business entity, then the authorized agent must be registered with the California Secretary of State to conduct business in California.

We may deny a request from an authorized agent if the agent cannot meet the above requirements. Further, before responding to a request from an authorized agent, we will still

require the authorized agent provide us with enough information so that we can verify your identity.

You may also make a verifiable consumer request on behalf of your minor child.

### **How often can you submit requests?**

You may only make a verifiable consumer request to know, obtain a copy, or delete your personal information twice within a 12-month period.

### **How do we verify requests?**

Before fulfilling your request, we take steps to verify you are who you say you are or that you have authority to act upon someone else's behalf. Therefore, upon receipt of your request, we may request additional information that we need to verify you and, if you are submitting a request on behalf of someone else, to verify that you are permitted to act on that person's behalf.

When we contact you to request verification information, please respond and provide the information that we have requested. Depending on the nature of the request you make, we may require you to verify your identity to either a "reasonable degree of certainty" or "high degree of certainty". This means that we need to match two or three pieces of information that we hold about you with information that you provide to us. This data could include, but is not limited to, email address, mailing address, phone number, trip/quote number, pickup address or drop off address.

In some cases, we may require you to sign a declaration under penalty of perjury that you are the consumer whose personal information is the subject of the request or that you are authorized to make the request on behalf of someone else.

In addition to providing the information we need to verify you or your authority, you must provide us with enough information so that we can understand, evaluate, and respond to your request. We cannot respond to your request or provide you with personal information if we cannot confirm the personal information relates to you.

We will only use personal information provided in the request to verify the requestor's identity or authority to make it.

### **Response timing and format**

We will confirm receipt of your request within ten (10) business days. If you do not receive confirmation within the 10-day timeframe, please contact us at: [USPrivacy@FirstGroup.com](mailto:USPrivacy@FirstGroup.com).

Our goal is to respond to a verifiable consumer request within 45 days of its receipt. If we need more time (up to another 45 days), we will let you know of the reason and extension period in writing within 45 days of receiving your verifiable consumer request.

Any disclosures we provide will only cover the 12-month period preceding our receipt of your request. The response we provide will also explain the reasons we cannot comply with a request, if applicable. When you request a copy of your personal information, 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 easily.

We do not charge a fee to process or respond to your verifiable consumer 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.

### **Personal information sales opt-out and opt-in rights**

To exercise the right to opt-out, you (or your authorized representative) may submit a request to us by visiting the following Internet Web page link.

[DO NOT SELL MY PERSONAL INFORMATION](#)

If you change your mind, the link can also be used to opt back into personal information sales.

Some browsers have signals that may be characterized as do not track signals, but we do not understand them to operate in that manner or to indicate a Do Not Sell expression by you, so we currently do not recognize these as a Do Not Sell request. We understand that various parties are developing do not sell signals and we may recognize certain such signals in the future.

Instead of opting out of the "sale" of your personal information, you may alternatively exercise more limited control of your personal information by instead exercising one of the following options:

- Opting out of promotional emails from us.
- Opting out of personalized advertising.

Information on how to opt out of promotional emails and opt out of personalized advertising can be found in our [Privacy Policy](#).

## **Non-Discrimination**

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

## **Other California privacy rights**

### **Third party marketing**

California's "Shine the Light" law (Civil Code Section § 1798.83) permits users of our website who are California residents to request certain information regarding our disclosure of personal information to third parties for their direct marketing purposes.

We do not currently make these types of disclosures.

### **Do Not Track**

When you visit our online services, we and third parties may use tracking technologies to collect usage information based on your

device for a variety of purposes, including serving you advertising, based on your having visited our services or your activities across time and third-party locations. Some browsers may enable you to turn on or off a so-called “Do Not Track” signal. Because there is no industry consensus on what these signals should mean and how they should operate, we do not look for or respond to “Do Not Track” signals.

## Contact us

Please contact us directly with any questions or concerns you may have about your privacy practices or if you are a consumer with a disability and need a copy of this notice in an alternative format.

You may reach our privacy office by:

- Calling us at 1-844-930-1776.
- Emailing us at [USPrivacy@FirstGroup.com](mailto:USPrivacy@FirstGroup.com) or [CanadaPrivacy@FirstGroup.com](mailto:CanadaPrivacy@FirstGroup.com) (Canada)

- Writing to us at:

FirstGroup America, Inc.,  
600 Vine Street  
Suite 1400  
Cincinnati, Ohio 45202  
Attention: North American Privacy  
Office