EFFECTIVE OCTOBER 10, 2023

California Residents Doing Work For AT&T

Recent Updates

Those California Residents Who Have Provided or Pursued Work at AT&T

If you live in California and have a work relationship with AT&T, you have certain rights under California law for your personal information in our possession. These rights are for employees, contractors and job applicants – either current or former. You can do the following: request access to your personal information, ask us not to sell or share it, ask us to delete it, or limit the use and sharing of sensitive personal information.

However, we do not sell or share the Personal Information or Sensitive Personal information of those who pursue or provide work for us. You can learn more by viewing our Privacy Notice for California Residents Doing Work for AT&T in the following section.

Click on the blue buttons below to submit a request to access, delete or correct personal information.

Access or Delete →

Correct →

Track a Request (https://www.att.com/mydatarequest/employee/inquiryverification)

Privacy Notice for California Residents Doing Work for AT&T

If you have a work relationship with AT&T, we must retain and process information about you. This lets us run the business and manage our relationship with you effectively, lawfully and appropriately. We must process and retain information when you apply for work, while you're doing work for us, and when you no longer do work for AT&T. This can include information to comply with an employment or other contract or work agreement, to comply with any legal requirements such as health and safety and occupational health obligations, to protect the safety of our employees or company assets, and to pursue AT&T's legitimate business interests and to protect our legal position in the event of legal proceedings or as otherwise required by applicable law, court order or government regulation.

AT&T is committed to fulfilling our responsibilities in relation to collection, retention, use, and other processing of information about you. Your information will be processed only for lawful and appropriate purposes. AT&T has implemented measures designed to secure your information and to help prevent unauthorized or accidental access, deletion, or other misuse. AT&T will facilitate the exercise of your privacy rights under California law in an effective and transparent manner.

California provides rights regarding your Personal Information. Key definitions are explained in the following section.

Personal Information

Personal Information means information that identifies, relates to, describes, is reasonably capable of being associated with, is linked to or could be reasonably linked to, either directly or indirectly, an identified or identifiable individual or household.

Sensitive Personal Information

Sensitive personal information includes any private information that reveals any of the following: Personal identification numbers, including social security, driver's license, passport, or state ID card numbers.

Workforce Analytics

Workforce Analytics refers to certain employee data that may be pulled from platforms or tools on company systems and/or company-owned devices, which may be paired with certain internal AT&T business and HR-related data or data from external sources, to provide aggregate insights (about groups, not individuals) on employee headcount, work locations, work distribution, collaboration, engagement, productivity, and workforce effectiveness, among other things.

Much of the information we retain is **provided by workers**. But some may come from other **internal sources**, such as your manager, or **external sources**, such as previous employment or study references, medical professionals or tax, judicial or governmental authorities.

Categories of Personal Information Collected

Categories of Personal Information Collected

We have collected the following categories of Personal Information from workers:

Categories	Examples	Categories of Sources from which Personal Information is Collected	Purpose of Collection and Use
Identifiers	A real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, Social Security number, driver's license number, passport number or other similar identifiers	• Provided by workers • Internal sources • External sources	• To fulfill or meet the reason workers provided the information, like hiring and distributing paychecks, training, security and background checks • To administer and provide company benefits, including parental leave, health insurance, life and accident insurance • To enable data storage • To provide financial services

				• To provide employment verification • To create photo IDs for security and access • To conduct information technology administration • To enable employment evaluation and advancement • To administer voluntary employee programs such as employee resource group participation, health and wellness applications, self-identification programs and identity verification programs • For internal communications, service optimization, security purposes and safety programs

			• To perform employee engagement analysis and Workforce Analytics
Characteristics of Protected Classification under California or Federal law	Age, race, national origin, citizenship, marital status, medical condition, physical or mental disability, sex (including gender, gender identity, pregnancy or childbirth and related medical conditions), sexual orientation, veteran or military status	• Provided by workers • Internal sources • External sources	• To recruit and extend work offers • To administer and provide company benefits, including parental leave, health insurance, life and accident insurance • To provide financial services • To administer voluntary employee programs such as employee resource group participation, health and wellness applications, self-identification programs and identity verification programs • To perform

			• To perform employee engagement analysis and Workforce Analytics
Commercial information	Records of AT&T products or services purchased, obtained or considered, or other purchasing or consuming histories or tendencies. Any such consumer interactions with AT&T may also be subject to the AT&T Privacy Notice (att.com/privacy)	• Provided by workers • Internal sources • External sources	• To provide benefits • To offer commercial products and services • To perform employee engagement analysis and Workforce Analytics
Biometric information	Physiological and biological characteristics, or activity patterns used to extract a template or other identifier or identifying information, such as, fingerprints, faceprints, and voiceprints or other physical patterns, and sleep, health or exercise data	• Provided by workers	• To identify individuals, identity verification, detect and prevent fraud, and safety or other security purposes
Internet or other similar network activity	Browsing history, search history, information on interactions with websites, email, calendar and meeting applications, social	• Provided by workers • Internal	• To conduct information technology administration and security

	applications, social media, applications or advertisements on company owned devices such as VPN connections or messaging software	• Internal sources • External sources	operations • For service optimization and safety programs • For monitoring compliance with company policies, including the Code of Business Conduct and COU policy • To perform employee engagement analysis and Workforce Analytics
Geolocation data	Physical location or movements and office presence	• Provided by workers • Internal sources • External sources	• For service optimization and safety programs • To fulfill or meet the reason workers provided the information, like hiring and distributing paychecks, training, coaching, security and background checks • To offer com-

			mercial products and services • To perform employee engagement analysis and Workforce Analytics
Professional or employment-related information	Current or past job history or performance evaluations Compensation data Resumes and/or applications for work	• Provided by workers • Internal sources • External sources	• To fulfill or meet the reason workers provided the information, like hiring and distributing paychecks, training, security and background checks • To perform employee engagement analysis and Workforce Analytics
Inferences drawn from other personal information	Profile reflecting a person's preferences, characteristics, behavior or attitudes including collaboration preferences like time spent in online meetings or emails sent	• Provided by workers • Internal sources • External sources	• To conduct information technology administration and security operations • For internal communications, service

			optimization, security purposes and safety programs • For monitoring compliance with company policies, including the Code of Business Conduct and COU policy • To provide training • To perform employee engagement analysis and Workforce Analytics
Audio, electronic, visual, thermal or similar information	Video surveillance; audio recordings; photographs;	• Provided by workers • Internal sources • External sources	• To conduct information technology administration and security operations • For internal communications, service optimization, security purposes and safety programs • For monitoring

			compliance with company policies, including the Code of Business Conduct and COU policy • To enable employee performance evaluation and coaching
Education Information	Academic records, degrees and schooling	• Provided by workers • Internal sources • External sources	• To fulfill or meet the reason workers provided the information, like hiring, training and background checks • To recruit and extend work offers • To administer and provide company benefits, including tuition reimbursement • To perform employee engagement analysis and Workforce Analytics

Information We Shared About California Residents who have provided work for AT&T

Here is information about the Personal Information we have collected from California Residents who have provided work for AT&T over the past year and the purpose for which we shared it. Some companies may receive your Personal Information from us to perform services on our behalf. Your data is not sold to them. They are under contract to protect your information, and they are only permitted to use it as needed to perform services, such as healthcare, financial services or cloud storage. You can see the categories of information disclosed to them in the table we've provided.

Categories	**Collected or Created**	**Categories of Companies we've shared with**	**Purpose for Sharing**
Identifiers	Collected	• Health/Benefits Providers • Claims/Plan Administrators • Data Storage Providers • Financial Services Providers • Job Training Providers	• To provide health and other benefits • To enable data storage • To provide financial services • To provide job training • To enable employment verification and back-

		• Employment Verification Providers • Workforce Management Providers	ground checks • To provide work-force manage-ment services
Characteristics of Protected Classification Under State or Federal Law	Collected	• Health/Benefits Providers • Claims/Plan Administrators • Data Storage Providers • Financial Services Providers • Job Training Providers • Employment Verification Providers • Workforce Management Providers	• To provide health and other bene-fits • To enable data storage • To provide finan-cial services • To provide job training • To enable em-ployment verifi-cation and back-ground checks • To provide work-force manage-ment services
Commercial in-formation	Collected	• Data Storage Providers • Financial	• To enable data storage • To provide finan-

		Services Providers	cial services
Internet or Other Electronic Network Activity Information	Collected	• Data Storage Providers • Workforce Management Providers • Information Security Services	• To enable data storage • To provide workforce management services • To provide information security services
Geolocation Data	Collected	• Claims/Plan Administrators • Health/Benefit Providers • Employment Verification Providers • Workforce Management Providers • Financial Services Providers • Data Storage Providers	• To provide health and other benefits • To enable employment verification and background checks • To provide workforce management services • To provide financial services • To enable data storage
Inferences or audience segmen-	Collected and	• Health/Benefits	• To provide health

tation	Created	• Health/Benefits Providers • Claims/Plan Administrators • Financial Services Providers • Job Training Providers • Workforce Management Providers • Data Storage Providers	• To provide health and other benefits • To provide financial services • To provide job training • To provide workforce management services • To enable data storage
Audio, electronic, visual, thermal, or similar information	Collected	• Job Training Providers • Volunteer Organizations • Security Providers • Data Storage Providers	• To provide job training, evaluation and coaching • To administer voluntary employee programs such as employee resource group participation, health and wellness applications, self-identification programs and identity verification programs • For service optimization and

			safety programs • For monitoring compliance with company policies, including the Code of Business Conduct and COU policy • To enable data storage
Biometric information	Collected	• Health/Benefits Providers • Claims/Plan Administrators • Security Providers	• To provide health and other benefits • To enable identity verification, detecting and preventing fraud, and safety or other security purposes
Education Information	Collected	• Claims/Plan Administrators • Workforce Management Providers • Training Providers • Credit Reporting Agencies	• To enable hiring, tuition reimbursement, training and background checks • To enable data storage

		• Data Storage Providers	
Professional or employment-related information	Collected	• Health/Benefits Providers • Claims/Plan Administrators • Workforce Management Providers • Job Training Providers • Credit Reporting Agencies • Data Storage Providers • Financial Services Providers	• To provide health and other benefits • To fulfill or meet the reason workers provided the information, like hiring and distributing paychecks, training, security and background checks • To provide workforce management services • To enable data storage • To provide financial services

The Sensitive Personal Information We've Collected and the Purpose of its Collection and Sharing

Here is information about the Sensitive Personal Information we have collected from California Residents who have provided work for AT&T over the past year, the purpose for which we collected it, the types of

companies we've shared it with and why. AT&T does not sell Sensitive Personal Information.

Categories	**Purpose for collection**	**Categories of Companies we've shared with**	**Purpose for Sharing (Making available constitutes a share)**
Gov't IDs: social security, driver's license, state Identification card, or passport number	• To Provide Benefits • To Provide Financial Services including paycheck distribution • To fulfill or meet the reason workers provided the information, like hiring and distributing paychecks, training, security and background checks • To Provide Employment Verification	• Health/Benefits Providers • Claims/Plan Administrators • Financial Services Providers • Employment Verification Providers • Credit Reporting Agencies • Workforce Management Providers • Training Providers	• To provide health and other benefits • To provide financial services • To enable employment verification and background checks • To

	• To administer voluntary employee programs such as employee resource group participation, health and wellness applications, self-identification programs and identity verification programs		pro-vide work-force man-age-ment ser-vices • To pro-vide job train-ing
Financial accounts & credentials: account log-In, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account	• To Provide expense reimbursement • To offer commercial products and services • Payroll/direct deposit	• Not Shared	• Not Shared
Precise geolocation	• For service optimization and safety programs.	• Not Shared	• Not Shared
Demographic, Religious or occupational informa-			

of occupational information: racial or ethnic origin, religious or philosophical beliefs, or union membership	• To administer voluntary employee programs such as employee resource group participation, health and wellness applications, self-identification programs and identity verification programs • Workforce Analytics	• Workforce Management Providers (Aggregated Reports)	• To provide workforce management services
Content of Communications: • For Company Provided Wireless Devices only: The contents of an individual's Plain SMS text messages up to 48 hours and spam texts unless AT&T is the intended recipient of the communication. Learn more (https://about.att.com/privacy/StateLawApproach/california/ca-workers.html#). • For Company Provided communica-	• Network Operations • Security Operations • Workforce Analytics	• Not Shared	• Not Shared

tions applications:The subject line of an individual's email message, meeting titles and chat messages			
Biometric, Health or Sexual information: the processing of biometric Information for the purpose of uniquely identifying an individual; personal Information collected and analyzed concerning an individual's health; or c. personal Information collected and analyzed concerning an individual's sex life or sexual orientation	• To identify individuals, identify verification, detect and prevent fraud, and safety or other security purposes • To administer voluntary employee programs such as employee resource group participation, health and wellness applications, self-identification programs and identity verification programs	• Fraud prevention and authentication/identity verification entities • Security Providers	• To prevent fraud/provide identity verification and for safety and other security purposes

AT&T 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.

Your Right To Request Disclosure Of Information We Collect And Share About You

We are committed to ensuring that you know what Personal Information (PI) we collect. You can ask us for the following information:

- The categories and specific pieces of your PI that we've collected.
- The categories of sources from which your PI was collected.
- The purposes for collecting or sharing your PI.
- The categories of third parties with whom we shared your PI.

We are also committed to ensuring that you know what information we share about you. You can submit a request to us for the following additional information relative to the sharing of your PI:

- The categories of PI that we've shared with service providers who provide services for us, like processing your benefits; the categories of third parties to whom we've disclosed that PI; and the category or categories of PI disclosed to each third party.

AT&T does not sell your PI collected through our work relationship unless you give us your explicit permission to do so, like to learn about optional benefits and discounts from service providers.

AT&T does not share your PI or SPI for cross-context behavioral advertising.

To exercise your right to request the disclosure of your PI that we collect or share, either visit our Californians Doing Work For AT&T page or contact

or share, either visit our Californians Doing Work For AT&T page or contact us at (800) 597-8244. These requests for disclosure are generally free and are provided in a format that is portable in a readily usable format.

Your Right To Request The Deletion Of Personal Information

Upon your request, we will delete the PI we have collected about you, except for example, situations when that information is necessary for us to: provide you with a good or service that you requested; perform a contract we entered into with you; maintain the integrity and security of our systems; comply with or exercise rights provided by the law; or use the information internally in ways that are compatible with the context in which you provided the information to us or that are reasonably aligned with your expectations based on your relationship with us.

To exercise your right to request the deletion of your PI, either visit our Californians Doing Work For AT&T page or contact us at (800) 597-8244. Requests to delete your PI are generally free.

Your Right To Ask Us Not To Sell or Share Your PI

AT&T does not sell or share your PI or Sensitive Personal Information.

Your Right to Request Correction of Inaccurate Personal Information

You may request that that we correct inaccurate PI we have about you. When you request that we correct inaccurate information, we will ask you to provide documentation supporting the accuracy of the PI that is the subject of your request. In doing so, we will evaluate the totality of the data relating to the contested PI. We may deny your request if we

determine that the contested PI is more likely than not accurate based on the data provided. Whether or not we are able to honor your correction request, you will be notified that your request was processed or denied and why. To exercise this right or choice, either visit our Californians Doing Work for AT&T page or contact us at (800) 597-8244.

Your Right to View California Metrics for the Prior Calendar Year

You may review information about the company's California data requests for the prior calendar year by visiting the California metrics page when applicable.

Verification of Identity – Access or Deletion Requests

Password Protected Account. If you maintain, or are eligible to maintain, password-protected access with us, you may submit an access or deletion request by authenticating yourself with a password the way you normally would when you access our internal systems. You'll have to authenticate yourself again to access your data or complete deletion.

Former Accountholders and Non-Accountholders (without a Password Protected Account). If you do not have password protected access, we will ask you to verify your identity using our mobile verification process. This process may involve a one-time pin or the capture of an image of your identity document, such as your driver's license, and compares it to a self-photo you submit. We will only use this information to verify your identity. We will delete it after the time expires allowed by the applicable state laws to process and respond to your request.

If we cannot verify your identity, we will not be able to respond to your request. We will notify you to explain.

AUTHORIZED AGENTS

You may designate an authorized agent to submit requests on your behalf. Your agent will need a valid power of attorney or written permission signed by you. If the agent relies on written permission, we'll need to verify the agent's identity. We may also contact you directly to confirm the permission. Your authorized agent can submit your requests by calling us at (800) 597-8244.

We Don't Mind If You Exercise Your Data Rights

We are committed to providing you control over your PI. If you exercise any of these rights explained in this section of the Policy, we will not disadvantage you. You will not be denied or charged different prices or rates for benefits or services or provided a different level or quality of employment or services.

As a resident of California, your Personal Information will be stored for a period of time consistent with applicable law and we keep your information as long as we need it for business, tax or legal purposes. AT&T decides how long to retain your Personal Information consistent with these criteria:

- The type of personal information collected;
- How long the personal information is needed to operate the business or provide our Products and Services; and
- Whether the business is subject to contractual or legal obligations – such as ongoing litigation, mandatory data retention laws or government orders to preserve data relevant to an investigation.

We reserve the right to amend this privacy notice at our discretion and at any time. If you have any concerns about how your information is

processed, or need a version of this notice in a format more readily-accessible by you, you can contact: privacypolicy@att.com (mailto:privacypolicy@att.com).

Last updated: August 1, 2023

Read the prior version (/ecms/dam/csr/privacy-redesign/Privacy-Notice-for-CA-Residents-Doing-Work-for-ATT.pdf)

You may have some additional questions, so we've listed some common questions and answers below.

What actions can I take? +

If you are a California resident and have a work relationship with AT&T (as an employee, contractor or job applicant – current or former), you can:

- Ask to view the information we have about you.
- Ask us to delete information that's linked to you.

- Request a correction of inaccurate information about you.

Can anyone make these requests? +

These requests are available to California residents who are AT&T employees, contractors or job applicants – either current or former. You can submit a request online or by phone at 866-385-3193.

How long do requests to view my information take? +

We'll work as quickly as possible to share your report within 45 days. The turnaround time largely depends on the request, but we'll keep you updated if it will be longer than 45 days.

What information does AT&T have about me? +

We use information Provided by workers, your supervisors and your departments to run the business. However, we do not share or sell information about you, including sensitive personal information.

Here's some of the data we may have:

- Information you've given us, like your home address and job application.
- Demographic information like your age, race and gender.
- Work location, salary, pay, training and evaluation details.

- Data generated by your use of company-owned systems, devices and vehicles.

Most importantly, we use strong safeguards to keep your data safe and secure. Want to know more about the data we have and how we use it? Learn more at the Privacy Center (https://about.att.com/privacy/StateLawApproach/ccpa.html).

What happens when I ask for my data to be deleted? +

We'll work as quickly as possible to process your request within 45 days and will let you know if we need more time. Keep in mind that California law allows us to keep data for things like:

- Running the business, including data necessary for your employment.
- Security and fraud protection.
- Compliance with legal obligations.