

COMMSCOPE PRIVACY NOTICE FOR CALIFORNIA EMPLOYEES AND CONTRACTORS

CommScope (the “Company”) collects and uses the Personal Information (defined below) of its current, former, and prospective employees, and contractors (collectively, the “Company Workforce”) as set forth in this Privacy Notice (defined below). The Company is respectful of such information and is committed to protecting it in line with applicable data protection laws. Data protection legislation regulates the ways in which your Personal Information is collected, used, and disclosed.

This Privacy Notice (“Privacy Notice”) provides the Company Workforce with information about the categories of Personal Information the Company collects, the length of time the Company intends to retain each category of Personal Information, the categories of sources from which Personal Information is collected, the purposes for which the Company processes that Personal Information, and the categories of third parties to which the Company may disclose such Personal Information.

When referred to in this Privacy Notice, the term “Personal Information” includes any information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual or household, including any information that is subject to the California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100 *et seq.* (“CCPA”) and the implementing regulations (collectively, “CCPA”).

1. The Personal Information Collected by the Company

The categories of Personal Information that the Company may process includes, but is not limited to, your:

- Identifiers – Name, home address, e-mail address, telephone number (including personal mobile number) and other contact information, images/photographs, details regarding military service, and other recruitment information submitted as part of the application process;
- Protected classifications – Age, date of birth, gender, disability, family composition (including marital status or partnership, names of spouse and/or dependants and/or next of kin and relationship);
- Family – Nominated beneficiaries, and emergency contact details;
- Education information – Educational and vocational training and history (including professional qualifications, grades, attendance at educational establishments and training received), student status, spoken/written/reading language proficiency, and details of other relevant skills;
- Professional or employment-related information – Status of employment, performance ratings, work time/utilization records, training records, evaluations, holiday or annual leave arrangements, terms of labor contract, details of any disciplinary actions, employee benefit plan participation details, stock option grants, grant number and type and value, employee number, company ID number, business title/unit/department/location, job position/title, functions and description, working arrangements (full/part-time), job location(s), seniority data, retirement timeline, contract length, hire/re-hire/termination date and codes, supervisor hierarchy, line management details, work history and experience, business travel arrangements, details of mobility/willingness to relocate, workplace accident information, occupational health information, development plans, salary information, expense reimbursement, benefit information (e.g., employer health insurance program), 401k, and stock option information (stock grants or option exercise details), bonus, additional pay, variable

compensation awards, tax data (national and local), flexible spending enrollments, grant valuation information, paid time off and credit card details (personal and business);

- Internet or other similar network activity – user IDs, IP addresses, and system logs;
- Sensitive Personal Information – Social Security Number, driver license number, or other government-issued identification number, work authorization/eligibility/ permit/visa requirements/status, citizenship/immigration information, background checks (including motor vehicle reports), and health and medical information about you and your spouse and children, bank account details, direct deposit/credit arrangements, health and safety data.

2. Purpose and Uses for Collecting Your Personal Information

The Company collects data from its employees only for the purpose of your employment relationship with the Company, including recruiting, hiring, onboarding, pre-employment testing, employee management and oversight, and benefits administration.

The Company may process your Personal Information in connection with your employment or, if you are a contractor, contract with the Company, or to further our legitimate interests related to the Company’s business operations.

Type of Personal Information	Purpose/Use
<ul style="list-style-type: none"> • Personal Identifiers and contact information including first and last name, mailing address, unique personal identifier, email address, telephone number, and user account name. • Protected classifications such as age, date of birth, gender, family composition (including marital status or partnership, names of spouse and/or dependents and/or next of kin and relationship • Biometric information, 	<ul style="list-style-type: none"> • To enforce our Website Terms of Use and other legal terms and policies; • To protect our and others’ interests, rights, and property (such as to protect our copyrighted materials); and • To comply with applicable legal requirements, such as tax and other government regulations and industry standards, contracts, and law enforcement requests. • For recruitment, appraisals, performance, promotion, training, discipline, grievances, complaints, and termination of your employment, administration, reporting, management and resource planning, pay and remuneration, pension and insurance and other benefits, tax, other deductions from pay, health and

<p>including fingerprints</p> <ul style="list-style-type: none"> • Sensitive Personal Information including social Security Number, driver license number, or other government-issued identification number, work authorization/eligibility/permit/visa requirements/status, citizenship/immigration information, background checks 	<p>safety, discipline, grievances and termination of your employment to:</p> <ul style="list-style-type: none"> • (i) ensure compliance with legal and regulatory requirements and Company policies (such as anti-bribery, corruption, tax, and social security requirements, the Company Workforce’s right to work, and litigation and other legal proceedings); and • (ii) comply with contractual obligations for administration, reporting and management, and resource planning. • The Company may collect, store, and use and/or transmit biometric data during the course of conducting Company operations/workforce management. Biometric data is collected, stored, used, and/or transmitted solely for identity verification, workplace security, and fraud prevention specifically in regard to “Timeclocks.” The Company will not sell, lease, or trade any biometric data that it receives from employees.
--	--

3. How Long the Company Retains Your Personal Information

The Company will retain your Personal Information for as long as it is necessary to complete the purpose for which it was collected. Personal Information collected for purposes related to employment (including recruiting, management, benefits, etc.) will be retained for as long as you are employed with the Company and then for a period of time after your employment has ended. That period of time depends and varies based on the categories of Personal Information, the purposes for which it was collected, and the laws that apply.

4. With Whom the Company Discloses Personal Information

The Company works with third party vendors and service providers to achieve the purposes for which the data was collected (e.g. insurers, legal and other professional advisers, company credit card providers, pension plan administrators) to provide employment/related benefits, for legal/regulatory purposes, or where the Company has another legitimate business purpose to do so. The Company prohibits these third parties from using or disclosing your Personal Information except as necessary to perform services or to comply with legal requirements. The Company, however, does not sell your Personal Information or disclose your Personal Information for purposes of cross-context behavioural advertising.

If we do disclose your Personal Information to any third-party service provider, those third parties fall into one of the following categories:

- Workforce management and human resource management providers;
- Operating Systems and Platforms;
- Government Entities;
- Customer Support Providers;
- Health & Safety Providers;
- Internet Service Providers;
- Financial Services Providers;
- Insurance Providers;
- Social Networks;
- Technology Providers;
- Cybersecurity Providers; and
- Supply Chain Management Providers.

Your Personal Information may be shared across the Company and its affiliates, where necessary, for our business purposes or to comply with applicable legal requirements.

The Company may also disclose your Personal Information: (1) as permitted by law or required by legal process; (2) to law enforcement authorities or other government officials; (3) when the Company believes disclosure is necessary or appropriate to prevent physical harm or financial loss or in connection with an investigation of suspected or actual illegal activity; (4) to seek advice from external counsel or in connection with litigation with a third party; or (5) in connection with the sale, purchase, or merger of its business (including a transfer of its assets).

5. Knowledge of Unauthorized Disclosure

Any employees who have knowledge of an impending unauthorized disclosure, whether intentional or unintentional, and who fail to act to prevent the unauthorized disclosure may be subject to discipline as described in the Enforcement section below and/or as otherwise described in the employee handbook.

6. Enforcement

All employees having care over or access to employee Personal Information must comply with the policies, procedures and practices described in this Privacy Notice. Any breach of any term or condition of this Privacy Notice, whether intentional or unintentional, is grounds for disciplinary action.

7. Children

We may collect data about children that are under 16 years old as necessary to provide and administer employment benefits and/or to otherwise comply with applicable laws. We do not sell the Personal Information of consumers under 16 years of age or disclose the Personal Information of consumers under 16 years of age for purposes of cross-context behavioral advertising.

8. Changes to this Privacy Notice

We may change this Privacy Notice at any time and will update the “Last Updated” date accordingly. If we make material changes, we will notify you via email at the email address we have on file for you.

9. Rights regarding your Personal Information

If you are a California resident, you may have the following rights regarding your Personal Information:

Right to Know and to Access

Subject to certain exceptions, and legal obligations, you have the right to request that we disclose certain information to you about our collection and use of your Personal Information, including whether we sell your Personal Information or disclose your Personal Information for cross-context behavior advertising purposes. You also have the right to request access to Personal Information collected about you and information regarding the categories of Personal Information; the categories of sources of that information; the business or commercial purposes for which we collect it; the third parties to whom we sell, share, or disclose it; and the specific pieces of Personal Information we collected about you.

This information is disclosed in the “Personal Information Collected by the Company” Section of this Privacy Notice. You may also submit a request for this information as described below. To protect your Personal Information, we may take steps to verify your identity before we act on your request.

Right to Portability

You have the right to request that we provide a copy of the Personal Information we have collected about you, in a portable and, to the extent technically feasible, readily usable format that allows you to transmit the data to another entity without hindrance. This right is subject to certain exceptions, and legal obligations imposed by state or federal privacy and employment laws. Once we receive your request and confirm your identity, we will provide to you a copy of your data as required under the applicable data protection laws. We may provide this data to you via email to the email address you have provided with your request.

Right to Delete

You have the right to request that we delete your Personal Information. This right is subject to certain exceptions, and legal obligations imposed by state or federal privacy and employment laws. 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.

Right to Correct Inaccurate Information

Subject to certain exceptions, and legal obligations imposed by state or federal privacy and employment laws, you have the right to request that we correct inaccurate Personal Information that we have collected about you. Once we receive your request and confirm your identity, we will review your request, taking into account the nature of the Personal Information and the purposes of the processing of the Personal Information to see if we can correct the data. We may also request additional information showing that the information you want to correct is inaccurate.

Right to Opt-Out of the Sale or Sharing of Personal Information to Third Parties

You have the right to opt-out of the sale or sharing of your Personal Information by the Company to third parties. Under California law, “sell” means to sell, rent, release, disclose, disseminate, make available, transfer, or otherwise communicate orally, in writing, or by electronic or other means your Personal Information to a third party for monetary or other valuable consideration. “Share” means sell, rent, release, disclose, disseminate, make available, transfer, or otherwise communicate orally, in writing, or by electronic or other means your Personal Information to a third party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration. We do not sell or share your Personal Information, as those terms are defined under California law.

Non-Discrimination or Retaliation

We will not discriminate or retaliate against you for exercising any of your data privacy rights.

How to Submit a Request

You or an authorized agent may submit a request to exercise your rights through one of two means:

- (1) By submitting a request via email to your HR Management at Phyllis.Walker@commscope.com or Tyler.Scannella@commscope.com; or
- (2) By submitting a request via Company’s privacy policy at this link: <https://www.commscope.com/about-us/privacy-policy/>.

Verification Procedures

In order to process your request to exercise your rights, we must first verify it using information necessary to complete your request. We do this by asking you to:

- (1) Provide personal identifiers we can match against information we may have collected from you previously; and
- (2) Confirm your request using the email and/or telephone account stated in the request.

We will not collect additional Personal Information from you for the sole purpose of your exercising your rights under the data protection laws.

Authorized Agent

You may authorize another individual or a business to make requests regarding your data privacy rights on your behalf. We may ask the individual to submit documentation or proof supporting their

authority to represent you, and we may ask you to either verify your own identity or confirm that you provided the authorized individual to act on your behalf.

Right to Limit Use and Disclosure of Sensitive Personal Information

You have the right to direct us to limit our use of your Sensitive Personal Information to that use which is necessary to perform the services or provide the goods reasonably expected by an average consumer who requests those goods or services. California law considers the following pieces of Personal Information to be “sensitive:” social security number, driver’s license number or other government-issued identification number, financial account number, any health insurance or medical identification number, an account password, security questions and answers, or unique biometric data. We use Sensitive Personal Information only as it is necessary to perform the services for which it was collected, as described in this Privacy Notice.

10. Questions or Concerns About Your Personal Information

If you have any concerns regarding the processing of your Personal Information as described throughout, please contact either Phyllis Walker (Phyllis.Walker@commscope.com) or Tyler Scannella (Tyler.Scannella@commscope.com). The Company will take appropriate steps to address any inquiries or complaints. The Company also cooperates with relevant data protection authorities for complaints concerning its handling of your Personal Information.

Effective Date: March 2026