ASSOCIATES VISITING FROM OUTSIDE THE U.S.

Please visit https://www.victoriassecretandco.com/our-company/associates/associate-privacy-policies to view privacy policies for associates in jurisdictions outside the US.

U.S. ASSOCIATE PRIVACY POLICY (*This Policy was last updated on October 3, 2022. Effective date January 1, 2023.)*

Victoria's Secret & Co., including its subsidiaries and affiliated entities (the "Company," "we," "us," or "our"), respects your concerns about privacy. This Internal Employee Privacy Policy ("Policy") explains what personal information we collect when you become an associate of the Company, how we use that information, to whom we disclose it, and how we safeguard personal information.

WHAT DOES THIS POLICY COVER?

This Policy applies to our employees who reside and work in the United States.

We may obtain the following categories of personal information about you (collectively, "employee personal information"):

- Contact information, including name, work and personal address, phone number, email address, and emergency contact information;
- Demographic and family information, including age, date of birth, race, gender, ethnicity, marital and family status, disability status, veteran status, and dependent information;
- Identification information, including driver's license or state identification card number, passport number, visa ID number, Social Security number, Social Insurance number, Tax ID number, Employee ID, and signature;
- Photographs, and video and audio recordings;
- Compensation, benefits, and payroll information, including bank account details and salary-related information, payment card information, tax-related information, and information relating to participation in group insurance policies (such as insurance policy number, medical information and health insurance information);
- Information relating to your position, including job title, job description, office location, hire date, termination date, training details, performance evaluation, disciplinary actions, information regarding fitness for work, paid time off or leave of absence, alcohol or drug testing-related information (where permitted by applicable law), and information regarding immigration status and eligibility for work;
- Information related to employment, including occupation details, CV information, education details, language and other job-related skills, historical compensation details, previous employment details, and references;

- Geolocation data;

- Information about your use of Company IT and communications resources, including timestamp information, IP address, activity logs, and call detail; and

- The content of communications that traverses Company IT and telecommunications resources.

WHEN IS EMPLOYEE PERSONAL INFORMATION COLLECTED, AND HOW IS IT USED?

If you're hired for a position with the Company, we will collect employee personal information during and after the course of your employment with us and use it to administer the employment and post-employment phases of the relationship.

We may incorporate information from your job application into your personnel file, and we may collect employee personal information directly from you. We also collect employee personal information in the course of job-related activities.

We may collect information from third parties (e.g., during the application and recruitment process, in connection with background checks and the onboarding process, and as part of a change in duties or a promotion) to supplement your employee personal information.

We may also collect and use contact information that you provide about people you know (for example, your emergency contacts or people covered by your benefits programs).

We may use your personal information for the following purposes:

- Workforce management: managing work activities and personnel generally, including recruiting and employee on-boarding; performing background checks; determining suitability for employment or promotion; determining physical and/or mental fitness for work; reviewing and evaluating performance; determining eligibility for and processing salary increases, bonuses, and other incentive-based compensation; providing employee discounts; providing references; managing attendance, absences, leaves of absences, and vacations; administering payroll and compensation services; reimbursing expenses; administering health, dental, and other benefits; training and development; making travel arrangements; securing immigration statuses; monitoring staff; creating staff directories; investigating suspected misconduct or non-performance of duties; managing disciplinary matters, internal investigations, grievances, and terminations; reviewing staffing decisions; and providing access to facilities;

- Facilities and emergencies: ensuring business continuity; protecting the health and safety of our staff and others; responding to incidents; safeguarding, monitoring, and maintaining our IT infrastructure, telecommunications network, office equipment, facilities, and other property; detecting or preventing theft or fraud, or attempted theft or fraud; and facilitating communication with you and your designated contacts in an emergency;

- Business operations: operating and managing our IT, communications systems and facilities, and monitoring the use of these resources; providing technical support;

performing data analytics; improving our services; allocating and managing company assets and human resources; strategic planning; producing promotional videos; managing projects; planning events; compiling audit trails and other reporting tools; maintaining records relating to business activities, budgeting, and managing finances; managing mergers, acquisitions, liquidations, sales, reorganizations or disposals, and integrating with purchasers; and

- Legal and compliance: complying with legal requirements, such as tax, record-keeping and reporting obligations; conducting audits, management and resolution of health and safety matters; complying with requests from government or other public authorities; responding to legal process such as subpoenas and court orders; pursuing legal rights and remedies; defending litigation and managing internal complaints or claims; conducting investigations; and complying with internal policies and procedures.

We may also use monitoring, communications interception, and recording technology to collect information about you and others to protect people and property. For example, we may use video and surveillance technology in our stores and in our facilities; and we may intercept, access, use, and disclose communications (like email) that traverses our company network and assets (e.g., computers and phones).

WHAT INFORMATION DO WE SHARE WITH OTHER ENTITIES (OR WHAT INFORMATION MAY THEY ACCESS BECAUSE OF THE SERVICES THEY PROVIDE)?

We may share your employee personal information (as listed above in "What Does this Policy Cover?") with our subsidiaries and affiliates. We may also share and/or transfer your employee personal information (as listed above in "What Does this Policy Cover?") with third-party service providers that provide us with services that we find necessary to run our business, and which may directly or incidentally involve your employee personal information. These providers help us do all the things listed above (see When is Employee Personal Information Collected and How is It Used?), as summarized below:

- Provide workforce management.
- Maintain facilities and respond to incidents and emergencies.
- Maintain business operations.
- Deliver legal and compliance services.

We also may disclose personal information about you (a) if we are required to do so by law or legal process (such as a court order or subpoena); (b) in response to requests by government agencies, such as law enforcement authorities; (c) to establish, exercise, or defend our legal rights; (d) when we believe disclosure is necessary or appropriate to prevent harm or financial loss; (e) in connection with an investigation of suspected or actual illegal activity; or (f) otherwise with your consent.

We reserve the right to share and/or transfer your information in the event we sell and/or transfer all or a portion of our business assets (including, without limitation, in the event of a merger, acquisition, joint venture, reorganization, dissolution or liquidation).

HOW DO WE PROTECT EMPLOYEE PERSONAL INFORMATION?

We maintain administrative, technical and physical safeguards designed to protect employee personal information from accidental, unlawful or unauthorized destruction, loss, alteration, access, disclosure, or use.

WHAT IF I HAVE QUESTIONS OR CONCERNS?

If you have questions or concerns about your employee personal information or this Privacy Policy, please contact**:**

ATTN: Privacy Matter
Victoria's Secret & Co. Legal Department
4 Limited Parkway
Reynoldsburg, OH 43068 US
VSPrivacy@victoria.com

UPDATES TO THIS POLICY

This Policy may be updated periodically to reflect changes in our personal information practices.

Supplemental Privacy Notice for California Employees

This Supplemental Privacy Notice (the "Notice") supplements the Internal Associate Privacy Policy. This Notice describes the types of personal information we collect about California residents who are (1) Company employees, owners, directors, officers and contractors (collectively "Company Personnel"), (2) emergency contacts of Company Personnel, or (3) individuals related to Company Personnel for whom Company administers benefits (collectively with Company Personnel, "HR Covered Individuals").

Company Personnel are responsible for providing this Notice to any HR Covered Individual whose personal information is provided to the Company by Company Personnel. Certain terms used in this Notice have the meanings given to them in the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020, and its implementing regulations (collectively, the "CCPA/CPRA").

Collection and Use of Personal Information

The Company may collect (and may have collected during the 12-month period prior to the effective date of this Notice) the following categories of personal information about HR Covered Individuals:

- **Identifiers:** identifiers, such as real name, alias, postal address, unique personal identifier (e.g., a device identifier, employee number, unique pseudonym, or user alias/ID), telephone number, online identifier, Internet Protocol address, email address, account name, Social Security number, driver's license number, passport number, and other similar identifiers

- **Additional Data Subject to Cal. Civ. Code § 1798.80:** signature, state identification card number, insurance policy number, education, bank account number, credit card number and

debit card number, and other financial information, medical information, and health insurance information

- **Protected Classifications:** characteristics of protected classifications under California or federal law, such as race, age, gender, sex, marital status, medical condition, disability, citizenship status, and military and veteran status

- **Online Activity:** Internet and other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding your interaction with websites or applications

- **Geolocation Data**

- **Sensory Information:** audio, electronic, visual, and similar information

- **Employment Information:** professional or employment-related information, such as compensation, benefits and payroll information (e.g., salary-related information, tax-related information, benefits elections and details regarding leaves of absence), information relating to your position (e.g., job title and job description), performance-related information (e.g., evaluations and training), talent management information (e.g., resumé information, occupation details, education details, certifications and professional associations, historical compensation details, previous employment details, and pre-employment screening and background check information, including criminal records information), emergency contact information, and dependent information

- **Education Information**

- **Inferences:** inferences drawn from any of the information identified above to create a profile about you reflecting your preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

The Company may use (and may have used during the 12-month period prior to the effective date of this Notice) the categories of personal information listed above for the purposes described in the Policy and for certain business purposes specified in the CCPA/CPRA, such as:

- Performing services, including maintaining or servicing accounts, providing service, processing or fulfilling orders and transactions, verifying HR Individuals' information, processing payments, providing financing services, providing analytics services, providing storage or providing similar services

- Helping to ensure security and integrity to the extent the use of your personal information is reasonably necessary and proportionate for these purposes

- Debugging to identify and repair errors that impair existing intended functionality

- Undertaking internal research for technological development and demonstration

- Undertaking activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by us, and to improve, upgrade, or

enhance the service or device that is owned, manufactured, manufactured for, or controlled by us

Collection and Use of Sensitive Personal Information

We also collect a subset of personal information that is deemed "sensitive personal information" under California law. The following describes the categories of sensitive personal information we collect and our purposes for collecting it. We do not sell or share for cross-context behavioral advertising sensitive personal information that we collected.

Categories of Sensitive Personal Information Collected	Purposes for which it is collected
Social security, driver's license, state identification card, or passport number.	• Comply with all applicable laws and regulations. • Conduct background checks (where permitted by applicable law) • Eligibility for employment • Business travel
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.	• For payroll processing and employee reimbursement.
Racial or ethnic origin, religious or philosophical beliefs, or union membership.	• To promote equal employment opportunities.
Contents of a mail, email, and text messages unless the business is the intended recipient of the communication	• Manage and monitor employee access to company facilities, equipment, and systems. • Investigate and enforce compliance with and potential breaches of Company policies and procedures. • Exercise or defend the legal rights of the Company and its employees and affiliates, customers, contractors, and agents.
Information concerning health	• Comply with all applicable laws and regulations. • Employee benefits administration • Workers' compensation claims management
Information concerning sex life or sexual orientation	• Employees may decide to join affinity groups related to sexual orientation; however, the company does not collect information regarding sexual orientation.

Retention of Personal Information

The Company retains personal information of HR Covered Individuals for the period reasonably necessary to achieve the purposes outlined in this Notice, unless a longer retention period is required or permitted by applicable law, taking into account relevant statutes of limitations and Company's records retention requirements and policies.

Sources of Personal Information

During the 12-month period prior to the effective date of this Notice, the Company may have obtained personal information about you from the following categories of sources:

- Directly from you
- Through your device
- Social networks
- Data analytics providers
- Government databases

Disclosure of Personal Information

During the 12-month period prior to the effective date of this Notice, the Company may have disclosed personal information about you to the following categories of third parties:

- Government entities
- Third parties in connection with corporate transactions, such as mergers, acquisitions, joint venture reorganization, divestitures, dissolution or liquidation.

During the 12-month period prior to the effective date of this Notice, the Company has not disclosed personal information for a business purpose to third parties.

The Company does not sell or share for cross-context behavioral advertising purposes any personal information about HR Covered Individuals.

California Privacy Rights

If you are an HR Covered Individual, you have certain choices regarding your personal information, as described below.

- **Access**: You have the right to request, twice in a 12-month period, that we disclose to you the personal information we have collected, used, or disclosed about you during the past 12 months.

- **Correction**: You have the right to request that we correct the personal information we maintain about you, if that information is inaccurate.

- **Deletion**: You have the right to request that we delete certain personal information we have collected from you.

- **Right to Non-Discrimination for Exercise of Privacy Rights**: Under the CCPA/CPRA, you have the right to not receive discriminatory treatment if you exercise your privacy rights under the CCPA/CPRA.

How to Submit a Request

To submit an access, correction or deletion request, please visit Your Data Rights or call us at 1-866-473-4728. To submit a request as an authorized agent on behalf of a HR Covered Individual, visit Your Data Rights**.** On the form, add your email address and information about the individual for whom you are submitting the request in the other required fields. Please add your name and phone number in the Request Details field and an indication that you are submitting the request as an authorized agent.

Verifying Requests

To help protect your privacy and maintain security, we will take steps to verify your identity before granting you access to your personal information or complying with your request. Upon submission, you will be required to provide your full name, date of birth and Employee ID. You will also be asked to verify the email address you submit with your request. You will receive an email from us with instructions on completing this step.

If you designate an authorized agent to make a request on your behalf, we may require you to provide the authorized agent written permission to do so and we may require you to verify your identity directly with us (as described above).

To the extent permitted by applicable law, we may charge a reasonable fee to comply with your request.