CCPA NOTICE AT COLLECTION FOR CALIFORNIA EMPLOYEES, INDEPENDENT CONTRACTORS, AND APPLICANTS

Last Updated: February 20th, 2025

VALENTINO USA Inc. (“**VALENTINO US**”, the “**Company**”, “**we**”, “**us**”, “**our**”) collects and uses (also through the activity of one or more designated data controllers as specified in the Privacy Policy), the personal information of its employees, independent contractors, and applicants for employment, including their sensitive personal information, for human resources, employment, benefits administration, health and safety, and other business-related purposes, including the business purposes listed in the charts below. We are committed to properly handling the personal information collected or processed in connection with your employment or contractual relationship with us. This Notice specifically relates to the personal information of California residents who are also our employees, independent contractors, or applicants for employment. This Notice does not form part of any contract of employment or other contract to provide services.

To view our full privacy policy, visit the following [LINK](https://www.valentino.com/en-us/help/customercare/legalarea/privacypolicy), or the section “Privacy Policy” as well as our Employee Handbook for further information related to Privacy.

**1. PERSONAL INFORMATION WE COLLECT**

We may collect the personal information and sensitive personal information categories listed in the tables below. The tables also list, for each category, its source, our expected retention period, and business or commercial purposes for such collection. We will not sell the personal information, including any sensitive personal information, we collect about our employees, independent contractors, or applicants for employment, nor will we share it with third parties for cross-contextual behavioral advertising.

|  |  |  |  |
| --- | --- | --- | --- |
| **CATEGORY OF PERSONAL INFORMATION** | **SOURCE** | **RETENTION PERIOD** | **BUSINESS OR COMMERCIAL PURPOSES FOR COLLECTION** |
| **Identifiers**, including information such as name, address, email address, signature | Directly from you; | 7 Years | Recruit and process employment applications, including verifying eligibility for employment and conducting background and related checks;  Conduct employee onboarding;  Maintain and administer payroll and employee benefit plans, including enrollment and claims handling;  Maintain personnel records and complying with record retention requirements;  Provide employees with human resources management services and employee data maintenance and support services;  Communicate with employees and their emergency contacts and plan beneficiaries;  Comply with applicable state and federal labor, employment, tax benefits, workers' compensation, disability, equal employment opportunity, workplace safety, and related laws;  Prevent unauthorized access to or use of the Company property, including information systems, electronic devices, network, and data;  Ensure employee productivity and adherence to Company policies;  Conduct internal audits and investigate complaints, grievances, and suspected violations of the Company’s policy;  Respond to law enforcement requests and as required by applicable law or court order;  Exercise or defend the legal rights of the Company and its employees, affiliates, customers, contractors, and agents. |
| **Commercial information**, including transaction information, purchase history, and financial data related to employee discount purchases. | Directly from you; | Purchases made within one State, using another State’s tax rate due to the purchase being sent to that State: 7 years.  Purchases made within one State: 5 years. | To monitor compliance with Company’s policies;  Respond to law enforcement requests and as required by applicable law or court order. |
| **Internet or other similar network activity information**, including all activity on the Company's information systems (such as internet browsing history, search history, intranet activity, email communications, stored documents and usernames and passwords for company systems) and all activity on the Company’s communications systems (such as call logs, voicemails, text messages, chat logs, app use, mobile browsing and search history, mobile email communications, and other information regarding an employee's use of company-issued devices). | Automated information collection from use of Company devices; | Browsing history, search history or internet activity: not retained  For users with Office 365 licenses: audit logs retained for **90 days** only for security-related activities. | Facilitate the efficient and secure use of Company information systems;  Ensure compliance with Company information systems policies and procedures;  Comply with applicable state and federal laws;  Prevent unauthorized access to, use, or disclosure or removal of the Company's property, records, data, and information;  Conduct internal audits and investigate complaints, grievances, and suspected violations of Company’s policy;  Exercise or defend the legal rights of the Company and its employees, affiliates, customers, contractors, and agents. |
| **Geolocation data**, such as the time and physical general location related to use of an internet website, application, or device | Directly from you;  Automated information collection from use of Company devices; | we No retention | Improve safety of employees, customers, and the public regarding use of the Company property and equipment;  Prevent unauthorized access, use, or loss of the Company property; |
| **Audio, electronic, visual, and similar information,** including call recordings, CCTV footage for safety and security purposes (e.g., office premises), and audio/video recordings of events, conferences, and meetings | Automated information collection from use of Company devices;  Directly from you. | No retention with the exception of CCTV which is retained for 3 months | Comply with applicable state and federal laws, including on workplace health and safety;  Prevent unauthorized access, use, or loss of the Company property;  Exercise or defend the legal rights of the Company and its employees, affiliates, customers, contractors, and agents. |
| **Professional or employment-related information**, such as employment application information (work history, academic and professional qualifications, educational records, references, and interview notes), background check, work authorization, performance and disciplinary records, salary, bonus, commission, and other similar compensation data, benefit plan enrollment, participation, and claims information | Directly from you;  Third parties, for example, job references, business partners, professional employer organizations or staffing agencies; | 7 Years | Recruit and process employment applications, including verifying eligibility for employment, background checks, and onboarding;  Design and administer employee benefit plans and programs, including for leaves of absence;  Maintain personnel records and comply with record retention requirements;  Communicate with employees and their emergency contacts and plan beneficiaries;  Comply with applicable state and federal labor, employment, tax, benefits, workers' compensation, disability, equal employment opportunity, workplace safety, and related laws;  Conduct internal audits and investigate complaints, grievances, and suspected violations of the Company policy;  Evaluate and provide useful feedback about job performance, facilitate better working relationships, and for employee professional development;  Exercise or defend the legal rights of the Company and its employees, affiliates, customers, contractors, and agents. |
| **Non-public education information**, such as education records, degrees and vocational certifications obtained, report cards, and transcripts | Directly from you; | 7 Years | Evaluate an individual's appropriateness for hire, or promotion or transfer to a new position at the Company. |

Sensitive personal information is a subtype of personal information consisting of specific and highly confidential information categories. We may collect or use information that falls within the sensitive personal information categories listed in the table below. We only use sensitive personal information for the business purposes described below.

|  |  |  |  |
| --- | --- | --- | --- |
| **CATEGORY OF SENSITIVE PERSONAL INFORMATION** | **SOURCE** | **RETENTION PERIOD** | **BUSINESS OR COMMERCIAL PURPOSES FOR COLLECTION** |
| **Government identifiers**, such as your Social Security number, driver's license, state identification card, and passport and visa information, and immigration status and documentation | Directly from you; | 7 Years | Recruit and process employment applications, including verify eligibility for employment and conducting background and related checks;  Process and administer payroll and employee benefit plans, including enrollment and claims handling;  Maintain personnel records and comply with record retention requirements;  Provide employees with human resources management services and employee data maintenance and support services;  Communicate with employees and their emergency contacts and plan beneficiaries;  Comply with applicable state and federal labor, employment, tax benefits, workers' compensation, disability, equal employment opportunity, workplace safety, and related laws;  Prevent unauthorized access to or use of the Company property, including information systems, electronic devices, network, and data;  Respond to law enforcement requests and as required by applicable law or court order. |
| **Complete account access credentials**, such as user names combined with required access/security code or password | Directly from you;  Automated information collection. | Deletion of data when the employee leaves the company | Provide employees with human resources management services and employee data maintenance and support services;  Prevent unauthorized access to or use of the Company information systems, electronic devices, network, and data;  Payroll and benefit administration services. |
| **Citizenship or immigration information** | Directly from you; | 7 Years | Comply with federal and state equal employment opportunity laws;  Verify employment eligibility (Form I-9). |
| **Health information**, including job restrictions and workplace illness and injury information | Directly from you;  Third parties, such as insurance companies, leave management companies. | 7 Years | Investigate and process workers' compensation claims;  Process health insurance claims. |

**2. PERSONAL INFORMATION WE HAVE COLLECTED IN THE PRECEDING TWELVE MONTHS**

In the preceding twelve months, we have collected the personal information and sensitive personal information categories listed in the tables below. The tables also list, for each category, its source, business or commercial purposes for collection, categories of third parties to whom we have disclosed such information, and the business or commercial purposes for such disclosure. We have not sold personal information in the preceding twelve months, including any sensitive personal information, we collected about our employees, independent contractors, or applicants for employment, nor have we shared it with third parties for cross-contextual behavioral advertising.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CATEGORY OF PERSONAL INFORMATION** | **SOURCE** | **BUSINESS OR COMMERCIAL PURPOSES FOR COLLECTION** | **CATEGORIES OF THIRD PARTIES WITH WHICH INFORMATION WAS DISCLOSED** | **BUSINESS OR COMMERCIAL PURPOSES FOR DISCLOSURE** |
| **Identifiers**, including information such as name, address, email address signature | Directly from you; | Recruit and process employment applications, including verifying eligibility for employment and conducting background and related checks;  Conduct employee onboarding;  Maintain and administer payroll and employee benefit plans, including enrollment and claims handling;  Maintain personnel records and complying with record retention requirements;  Provide employees with human resources management services and employee data maintenance and support services;  Communicate with employees and their emergency contacts and plan beneficiaries;  Comply with applicable state and federal labor, employment, tax benefits, workers' compensation, disability, equal employment opportunity, workplace safety, and related laws;  Prevent unauthorized access to or use of the Company property, including information systems, electronic devices, network, and data;  Ensure employee productivity and adherence to Company policies;  Conduct internal audits and investigate complaints, grievances, and suspected violations of the Company’s policy;  Respond to law enforcement requests and as required by applicable law or court order;  Exercise or defend the legal rights of the Company and its employees, affiliates, customers, contractors, and agents. | Service providers and contractors;  Affiliated companies;  Government or administrative agencies. | Administrative and operational purposes, on behalf of or jointly with the Company, such as payroll processing, benefits administration, background checks, IT support, facilities management, human resource management, training and development programs. |
| **Commercial information**, including transaction information, purchase history, and financial data related to employee discount and clothing allowance purchases. | Directly from you; | To monitor compliance with Company’s policies;  Respond to law enforcement requests and as required by applicable law or court order. | Service providers and contractors;  Affiliated companies. | Administrative and operational purposes, on behalf of or jointly with the Company, such as benefits administration, and business expenses reimbursement. |
| **Internet or other similar network activity information**, including all activity on the Company's information systems (such as internet browsing history, search history, intranet activity, email communications, stored documents and usernames and passwords for company systems) and all activity on the Company’s communications systems (such as call logs, voicemails, text messages, chat logs, app use, mobile browsing and search history, mobile email communications, and other information regarding an employee's use of company-issued devices). | Automated information collection from use of Company devices; | Facilitate the efficient and secure use of Company information systems;  Ensure compliance with Company information systems policies and procedures;  Comply with applicable state and federal laws;  Prevent unauthorized access to, use, or disclosure or removal of the Company's property, records, data, and information;  Conduct internal audits and investigate complaints, grievances, and suspected violations of Company’s policy;  Exercise or defend the legal rights of the Company and its employees, affiliates, customers, contractors, and agents. | Service providers and contractors;  Affiliated companies. | Administrative and operational purposes, on behalf of or jointly with the Company, such as IT support, human resource management, training and development programs, and security and integrity of IT systems. |
| **Geolocation data**, such as the time and physical general location related to use of an internet website, application, or device | Directly from you;  Automated information collection from use of Company devices; | Improve safety of employees, customers, and the public regarding use of the Company property and equipment;  Prevent unauthorized access, use, or loss of the Company property; | Service providers and contractors;  Affiliated companies. | Administrative and operational purposes, on behalf of or jointly with the Company, such as IT support, facilities management, and to protect Company’s assets. |
| **Audio, electronic, visual, and similar information,** including call recordings, CCTV footage for safety and security purposes (e.g., office premises), and audio/video recordings of events, conferences, and meetings | Automated information collection from use of Company devices;  Directly from you. | Comply with applicable state and federal laws, including on workplace health and safety;  Prevent unauthorized access, use, or loss of the Company property;  Exercise or defend the legal rights of the Company and its employees, affiliates, customers, contractors, and agents. | Service providers and contractors. | Administrative and operational purposes, on behalf of or jointly with the Company, such as facilities management, human resource management, protect Company’s assets. |
| **Professional or employment-related information**, such as employment application information (work history, academic and professional qualifications, educational records, references, and interview notes), background check, work authorization, performance and disciplinary records, salary, bonus, commission, and other similar compensation data, benefit plan enrollment, participation, and claims information | Directly from you;  Third parties, for example, job references, business partners, professional employer organizations or staffing agencies; | Recruit and process employment applications, including verifying eligibility for employment, background checks, and onboarding;  Design and administer employee benefit plans and programs, including for leaves of absence;  Maintain personnel records and comply with record retention requirements;  Communicate with employees and their emergency contacts and plan beneficiaries;  Comply with applicable state and federal labor, employment, tax, benefits, workers' compensation, disability, equal employment opportunity, workplace safety, and related laws;  Conduct internal audits and investigate complaints, grievances, and suspected violations of the Company policy;  Evaluate and provide useful feedback about job performance, facilitate better working relationships, and for employee professional development;  Exercise or defend the legal rights of the Company and its employees, affiliates, customers, contractors, and agents. | Service providers and contractors. | Administrative and operational purposes, on behalf of or jointly with the Company, such as benefits administration, background checks, training and development programs. |
| **Non-public education information**, such as education records, degrees and vocational certifications obtained, report cards, and transcripts | Directly from you; | Evaluate an individual's appropriateness for hire, or promotion or transfer to a new position at the Company. | Affiliated companies. | Administrative and operational purposes, on behalf of or jointly with the Company, such as human resource management. |

Sensitive personal information is a subtype of personal information consisting of specific and highly confidential information categories. In the preceding twelve months, we have collected or used information that falls within the sensitive personal information categories listed in the table below. We only use sensitive personal information for the business purposes described below.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CATEGORY OF SENSITIVE PERSONAL INFORMATION** | **SOURCE** | **BUSINESS OR COMMERCIAL PURPOSES FOR COLLECTION** | **CATEGORIES OF THIRD PARTIES WITH WHICH INFORMATION WAS DISCLOSED** | **BUSINESS OR COMMERCIAL PURPOSES FOR DISCLOSURE** |
| **Government identifiers**, such as your Social Security number, driver's license, state identification card, and passport and visa information, and immigration status and documentation | Directly from you; | Recruit and process employment applications, including verify eligibility for employment and conducting background and related checks;  Process and administer payroll and employee benefit plans, including enrollment and claims handling;  Maintain personnel records and comply with record retention requirements;  Provide employees with human resources management services and employee data maintenance and support services;  Communicate with employees and their emergency contacts and plan beneficiaries;  Comply with applicable state and federal labor, employment, tax benefits, workers' compensation, disability, equal employment opportunity, workplace safety, and related laws;  Prevent unauthorized access to or use of the Company property, including information systems, electronic devices, network, and data;  Respond to law enforcement requests and as required by applicable law or court order. | Service providers and contractors;  Affiliated companies. | Administrative and operational purposes, on behalf of or jointly with the Company, such as payroll processing, benefits administration, background checks, human resource management. |
| **Complete account access credentials**, such as user names combined with required access/security code or password | Directly from you;  Automated information collection. | Provide employees with human resources management services and employee data maintenance and support services;  Prevent unauthorized access to or use of the Company information systems, electronic devices, network, and data;  Payroll and benefit administration services. | Service providers and contractors;  Affiliated companies. | Administrative and operational purposes, on behalf of or jointly with the Company, such as payroll processing and benefits administration. |
| **Citizenship or immigration information** | Directly from you; | Comply with federal and state equal employment opportunity laws;  Verify employment eligibility (Form I-9). | Government and administrative agencies. | Regulatory compliance. |
| **Health information**, including job restrictions and workplace illness and injury information | Directly from you;  Third parties, such as insurance companies, leave management companies. | Investigate and process workers' compensation claims;  Process health insurance claims. | Service providers and contractors. | Benefit administration. |

**3. YOUR RIGHTS UNDER THE CCPA**

You have the right under the CCPA, to exercise, free of charge, the following rights:

1. Right to Know. You have the right to request information about the personal information we have collected about you, including the categories of personal information, sources of collection, and the business purposes for collecting it.

You have the right to request information about the personal information we sold, shared or disclosed, including the categories of personal information, the categories of third parties to whom the information was sold, shared, or disclosed, and the business purposes for collecting, sharing or disclosing it. Additionally, you have the right to request specific pieces of personal information in a portable and structured format.

1. Right to Correct. You can request the correction of inaccuracies in your personal information.
2. Right to Delete. In certain circumstances, you have the right to request the deletion or de-identification of your personal information. However, please note that this right does not apply in specific situations, such as when the information is necessary to provide services, fulfill a contract, protect security and rights, comply with legal obligations, or engage in research or other lawful uses.

**4. HOW TO EXERCISE YOUR RIGHTS**

To exercise your rights, described above, you can:

* call the number 212-997-8100 from Monday to Friday from 9:00am to 9:00pm (EST, excluding public holidays); or
* contact us directly at [privacy@valentino.com](mailto:privacy@valentino.com).

Please note that we can deny a CCPA-related data access or data portability disclosure request if you already made such a request twice within a 12-month period.

If you choose to contact us directly by phone or email, you will need to provide us with: (i) enough information to identify you; (ii) proof of your identity and address (e.g., a copy of your driving license or passport and a recent utility or credit card bill); and (iii) description of what right you want to exercise and the information to which your request relates.

We are not obligated to satisfy a request for a data access or data portability disclosure, or to correct personal information, if we cannot verify that the person making the request is the person about whom we collected information, or is someone authorized to act on such person’s behalf.

Any personal information we collect from you to verify your identity in connection with you request will be used solely for the purposes of verification.

You may designate an authorized agent to exercise your rights outlined above in Section 3. If you utilize an authorized agent to exercise a CCPA right, the following proof that the agent has been authorized to act on your behalf will need to be provided:

* Your written permission for the authorized agent to act on your behalf and separate verification of your identity; or
* Proof that the authorized agent holds a power of attorney to act on your behalf pursuant to Cal. Probate Code §§ 4121--4130.

**5. NO DISCRIMINATION**

If you choose to exercise any of your rights under the CCPA, you have the right to not receive discriminatory treatment by us.

**6. CONTACT US**

If you have any questions about this Notice or need to access this Notice in an alternative format due to having a disability, please contact hrusa@valentino.com

**7. CONSENT AND ACKNOWLEDGEMENT OF RECEIPT**

I hereby acknowledge receipt of this Notice from VALENTINO US and consent to VALENTINO US collecting and processing my personal information for the purposes described in this Notice.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name