

Job Applicant Privacy Notice

Effective Date: 2/8/2023

At ZocDoc, Inc. (the “Company,” “us” or “we”), we are committed to protecting the privacy and security of the personal information you provide to us. If you are one of our job applicants located in California, you have certain rights under the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 (“CPRA”), with respect to your personal information, as outlined below. Please read this Job Applicant Privacy Notice (the “Privacy Notice”) to learn how we treat your personal information when you apply for a job or other role with us. In this Privacy Notice, we use the term “personal information” as it is defined in the CPRA. This Privacy Notice only applies to job applicants who are residents of the State of California.

As we continually work to improve our operations and business, we may need to change this Privacy Notice from time to time. Upon such changes, we will alert you to any such changes by placing a notice on the Company’s intranet, by sending you an email, and/or by some other means.

What Categories of Personal Information Do We Collect?

This chart details the categories of personal information that we collect and have collected over the past twelve (12) months:

Category of Personal Information	Examples of Personal Information We Collect	Categories of Third Parties With Whom We Share This Personal Information
Identifiers	• Real name • Alias • Postal address • Unique personal identifier (including, telephone number or device identifier) or online identifier • IP address • Email address • Account name • Social security number • Driver’s license number or passport number • Other similar identifiers	• Service Providers
Categories of Personal Information Described in California Customer Records Act (Cal. Civ. Code § 1798.80(e))	• Name • Signature • Social security number • Physical characteristics or description • Address • Telephone number • Passport number, driver’s license or state identification card number • Insurance policy number • Educational information	• Service Providers

Category of Personal Information	Examples of Personal Information We Collect	Categories of Third Parties With Whom We Share This Personal Information
	• Employment or employment history • Bank account number, credit card number, debit card number or any other financial information • Medical information or health insurance information, including COVID-19-related information, such as: ○ your symptoms of COVID-19; whether you have been tested for COVID-19; any statements from you that you have COVID-19 or suspect you have COVID-19; our notes or other documentation from screening you about symptoms of COVID-19 or that result from any COVID-19 test that we provide; COVID-19-related doctors' notes pertaining to your absences from work or work limitations/restrictions, or certifying fitness to return to work, requests for accommodation and/or that you are receiving an accommodation; correspondences with you and/or your health care provider(s) regarding any of the foregoing; and our notes or other documentation in connection with your COVID-19 vaccination status (including, without limitation, proof of receipt of a COVID-19 vaccine).	
Characteristics of Protected Classifications under California or Federal Law	• Race • Religious creed • National origin • Ancestry • Physical or mental disability • Medical condition • Marital status • Sex, gender, gender identity, or gender expression • Age • Sexual orientation • Military and veteran status	• Service Providers
Commercial Information	• Records of personal property, products or services purchased, obtained, or considered	• Service Providers

Category of Personal Information	Examples of Personal Information We Collect	Categories of Third Parties With Whom We Share This Personal Information
Internet or Other Electronic Network Activity Information	• Information regarding your interaction with an internet website, application, or advertisement (including chats and instant messaging)	• Service Providers
Geolocation Data	• IP-address-based location information • GPS data	• Service Providers
Photos, Videos, or Recordings	• Photos, videos, or recordings of you • Photos, videos, or recordings of your environment	• Service Providers
Professional or Employment-Related Data	• Resume • Job title • Job history • Performance evaluations • Union membership • Job interview notes, responses to screening questions, and assessment results	• Service Providers • [Affiliates]
Education Information (as defined in the Family Educational Rights and Privacy Act (20 U.S.C. Sec. 1232g; 34 C.F.R. Part 99))	• Grades or transcripts • Student financial information • Student disciplinary records	• Service Providers
Categories of Personal Information Considered “Sensitive” Under the California Privacy Rights Act	• Social security, driver’s license, state identification card or passport numbers • 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 • Precise geolocation • Racial or ethnic origin • Religious beliefs • Philosophical beliefs • Union membership • Contents of your mail, email, and text messages where the Company is not the intended recipient of the communication • Biometric information for the purpose of uniquely identifying your ○ Personal information concerning your health (including facial	• Service Providers

Category of Personal Information	Examples of Personal Information We Collect	Categories of Third Parties With Whom We Share This Personal Information
	recognition information in connection with COVID-19 health screenings)	

Categories of Sources of Personal Information

We collect personal information from the following categories of sources:

- You
 - When you provide such information directly to us.
- Public Records
 - From the government or other sources.
- Third Parties. For example, we may collect information from:
 - Vendors
 - Recruiters.
 - Pre-employment screening services.
 - Credentialing and licensing organizations.
 - Consumer reporting agencies.
 - Prior employers (e.g., for references)
 - Professional references
 - Educational institutions
 - Publicly available Sources
 - Social networks, including your social media profile (e.g., LinkedIn, Twitter, and/or Facebook).
 - Other public sources you identify or refer us to.

Our Commercial or Business Purposes for Collecting or Disclosing Personal Information

- Recruiting and/or Hiring You and Operating, Hosting, and Facilitating Our Operations and Business
 - Processing and managing your application.
 - Conducting background and reference checks.
 - Providing immigration support.
 - Entering into contracts.
 - Implementing, managing, and improving the Company's recruitment process and diversity and inclusion programs.
 - Implementing health and safety measures and maintaining a safe workplace.
 - Managing the Company's relationship with you.
 - Meeting or fulfilling the reason you provided the information to us.
 - Maintaining the security of our systems and property, and doing fraud protection, security, and debugging.
 - Carrying out other business or employment-related purposes stated when collecting your personal information or as otherwise set forth in applicable data privacy laws, such as the CPRA.

- Meeting Legal Requirements and Enforcing Legal Terms
 - Fulfilling our legal obligations under applicable law, regulation, court order, or other legal processes, such as preventing, detecting, and investigating security incidents and potentially illegal or prohibited activities, or responding to lawful requests by public authorities, including to meet national security or law enforcement requirements.
 - Protecting the rights, property, or safety of you, the Company, or another party.
 - Enforcing any agreements with you.
 - Responding to claims.
 - Resolving disputes.

We 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.

How We Disclose Your Personal Information

We may disclose your personal information to the and/or for the purposes described in this section.

Service Providers

Service providers help us to perform business functions on our behalf. They may include:

- Professional advisors.
- Hosting, technology, and communication providers.
- Security and fraud prevention consultants.
- Background and reference check screening services.
- Hiring process management and administration tools.
- Health and safety technology providers (such as providers of telethermographic systems to measure body temperature), COVID-19 screening services, and COVID-19 testing providers.

Legal Obligations

We may share any personal information that we collect with third parties in conjunction with any of the activities set forth under “Meeting Legal Requirements and Enforcing Legal Terms” in the “Our Commercial or Business Purposes for Collecting or Disclosing Personal Information” section above.

Business Transfers

All of your personal information that we collect may be transferred to a third party if we undergo a merger, acquisition, bankruptcy, or other transaction in which that third party assumes control of our business (in whole or in part). Should one of these events occur, we will make reasonable efforts to notify you before your information becomes subject to different privacy and security policies and practices.

Information that is Not Personal Information

We may create aggregated, de-identified, or anonymized data from the personal information we collect, including removing information that makes the data personally identifiable to a particular job applicant. We may use such aggregated, de-identified, or anonymized data and share it with third parties for our lawful business purposes, including to operate, host, and facilitate our operations and business, provided that we will not share such data in a manner that could identify you.

Data Security

We seek to protect your personal information from unauthorized access, use, and disclosure using appropriate physical, technical, organizational, and administrative security measures based on the type of personal information and how we are processing that information. You should also help protect your data by appropriately selecting and protecting your password and/or other sign-on mechanisms, limiting access to your computer or device and browser, and signing off after you have finished accessing your account. Although we work to protect the security of your account and other data that we hold in our records, please be aware that no method of transmitting data over the internet or storing data is completely secure.

Data Retention

We retain personal information about you for as long as necessary to perform our business or commercial purposes, including employment-related purposes, for collecting your personal information. When establishing a retention period for specific categories of personal information, we consider who we collected the personal information from, our need for the personal information, why we collected the personal information, and the sensitivity of the personal information. In some cases, we retain personal information for longer, if doing so is necessary to comply with our legal obligations, resolve disputes, or is otherwise permitted or required by applicable law, rule, or regulation. If you are offered and accept a position of employment or engagement with us, the personal information collected during the application and recruitment processes will become part of your employment or personnel record, and we may use it in connection with your employment or engagement consistent with our policies applicable to our employees. If you do not become an employee of or are not otherwise engaged by us, or once you are no longer an employee of or engaged by us, we will retain and securely destroy your personal information in accordance with applicable laws and regulations, and the retention description identified herein or in our policies applicable to the personal information of our personnel. We may further retain information in an anonymous or aggregated form where that information would not identify you personally.

Job Applicant Rights

You have the rights set forth in this section. Please see the “Exercising Your Rights Under the CPRA” section below for instructions regarding how to exercise these rights. Please note that these rights may be subject to certain exceptions and exclusions as provided under the CPRA.

Access

You have the right to request certain information about our collection and use of your personal information over the past twelve (12) months. In response, we will provide you with the following information:

- The categories of personal information that we have collected about you.
- The categories of sources from which that personal information was collected.
- The business or commercial purpose for collecting or selling your personal information.
- The categories of third parties with whom we have shared your personal information.
- The specific pieces of personal information that we have collected about you.

If we have disclosed your personal information to any third parties for a business purpose over the past twelve (12) months, we will identify the categories of personal information shared with each category of the third party recipient.

Deletion

You have the right to request that we delete the personal information that we have collected about you. Under the CPRA, this right is subject to certain exceptions: for example, we may need to retain your personal information if deletion of your personal information involves disproportionate effort. If your deletion request is subject to one of these exceptions, we may deny your deletion request.

Correction

You have the right to request that we correct any inaccurate personal information we have collected about you. Under the CPRA, this right is subject to certain exceptions: for example, if we decide, based on the totality of circumstances related to your personal information, that such data is correct. If your correction request is subject to one of these exceptions, we may deny your request.

Processing of Sensitive Personal Information Opt-Out

We collect personal information that is considered “sensitive personal information” under the CPRA. Consumers have certain rights over the processing of their sensitive personal information. Please note that we only use or disclose your sensitive personal information for the purposes set forth in section 7027(m) of the CPRA regulations and we do not collect or process sensitive personal information with the purpose of inferring any characteristics about California residents.

Personal Information Sales Opt-Out and Opt-In

We will not sell your personal information and have not done so over the last twelve (12) months. To our knowledge, we do not sell the personal information of minors under sixteen (16) years of age.

Personal Information Sharing Opt-Out and Opt-In

Under the CPRA, you have certain rights when a business “shares” personal information with third parties for purposes of cross-contextual behavioral advertising. We will not share your personal information for cross-contextual behavioral advertising and have not done so over the last twelve (12) months. To our knowledge, we do not share the personal information of minors under sixteen (16) years of age for purposes of cross-contextual behavioral advertising.

We Will Not Discriminate Against You for Exercising Your Rights Under the CPRA

We will not discriminate against you for exercising your rights under the CPRA. Job applicants will not be subject to any retaliation or disciplinary action for exercising their rights under the CPRA.

Exercising Your Rights Under the CPRA

To exercise the rights described in this Privacy Notice, you or your Authorized Agent (defined below) must send us a request that (1) provides sufficient information to allow us to verify that you are the person about whom we have collected personal information, and (2) describes your request in sufficient detail to allow us to understand, evaluate and respond to it. Each request that meets both of these criteria will be considered a “Valid Request.” We may not respond to requests that do not meet these criteria. We will only use the personal information provided in a Valid Request to verify your identity and complete your request. You do not need an account to submit a Valid Request.

We will work to respond to your Valid Request within the time period required by applicable law. We will not charge you a fee for making a Valid Request unless your Valid Request(s) is excessive, repetitive, or manifestly unfounded. If we determine that your Valid Request warrants a fee, we will notify you of the fee and explain that decision before completing your request.

You may submit a Valid Request using the following methods:

- Email us at: Privacy@zocdoc.com
- Call us at: (855) 962-3621

You may also authorize an agent (an “Authorized Agent”) to exercise your rights on your behalf. To do this, you must provide your Authorized Agent with written permission to exercise your rights on your behalf, and we may request a copy of this written permission from your Authorized Agent when they make a request on your behalf.

Contact for Questions

If you have any questions or comments regarding this Privacy Notice, the ways in which we collect and use your personal information, or your choices and rights regarding such collection and use, please contact:

- Email us at: Privacy@zocdoc.com
- Call us at: (855) 962-3621

Job applicants with disabilities may access this Privacy Notice in an alternative format by contacting privacy@zocdoc.com, ZocDoc, Inc., 568 Broadway FL 9, New York, NY 10012 or (855) 962-3621.