

WESTERN DIGITAL APPLICANT PRIVACY NOTICE

Last Updated: April 1, 2026

Introduction

Western Digital Technologies, Inc. and its subsidiaries and affiliates (together “**Western Digital**,” “**we**,” “**us**” or “**our**”) is committed to protecting the privacy and security of your personal information. This Privacy Notice (“**Notice**”) describes what personal information we collect from Western Digital job applicants, the purposes for the collection, and to whom we may disclose your personal information.

This Notice applies only to the personal information of job applicants and candidates of employment, as well as those who may participate in recruiting programs and events. This notice does not form part of any contract of employment or other contract to provide services. For information about how we collect and use your information as a consumer, please review our [Privacy Center](#) at WesternDigital.com.

To submit a profile for a position with Western Digital, you must read this Notice and, depending on the applicable data protection laws where you reside, either acknowledge that you have received and understood it or consent to the terms of this Notice. If you do not either acknowledge that you have received and understood it or consent to this Notice, you will not be able to submit a profile for a position.

As used in this Notice:

- “Processing of personal information” means any operation performed on personal data, such as the collection, recording, storing, using, reviewing, disclosing, transferring, or deleting of personal information.
- “Personal information” means information relating to an identified or identifiable Western Digital applicant insofar as that information has been obtained by Western Digital in the context of the Western Digital’s applicant’s potential working relationship with Western Digital. The personal information we may process about you are detailed in the section “The Personal Information That Western Digital Collects”.

If you have any questions, you can reach out Western Digital’s Data Protection Officer (DPO) by email at privacy@wdc.com.

The Entity That Is Collecting Your Personal Information

The data controller of your personal information is the Western Digital entity you are interacting with as part of your application (i.e. either Western Digital Technologies, Inc. or one of its subsidiary or affiliate).

How Western Digital Collects Your Personal Information

Western Digital collects your personal information from a variety of sources, but mainly from you. You provide us your personal information when you apply for a job, and when you work for Western Digital as employee. For example, you create personal information when you interact with our information and communication systems. We will also receive personal information about you from your manager, co-workers, People Support, and other functions.

Western Digital also collects personal information about you from third parties but only if authorized or required by applicable local law. For example, and depending on the applicable local law where you reside, Western Digital may collect your personal information: recruiters, consumer reporting agencies, service providers, vendors, contractors, credit agencies, or service providers who provide services on our behalf.

Where legally permissible, we collect your personal information as part of a background check. Western Digital may verify your personal information and conduct reference checks and/or conduct background checks (if and to the maximum extent permitted by applicable local law) if you are offered a job.

WESTERN DIGITAL APPLICANT PRIVACY NOTICE

The Personal Information That Western Digital Collects

As part of the application process and unless prohibited by applicable local law, Western Digital requests and processes the following categories of personal information about you:

- **Identifiers**, such as your full name, preferred name, and any names you may have used in the past, home address, phone number, email address, Social Security number or other government issued identification number;
- **Professional and employment-related information**, such as the position you are applying for, your previous employer information, your previous work history, your references, your education and training history, work authorization requirements, the languages you speak, qualifications and certifications, your current compensation information (where provided by you at your sole discretion), as well as your compensation expectations salary or wage expectations, and any information included in your resume or CV, cover letter, and interview notes;
- **Geolocation data**, such as your zip code, the time and physical location related to use of our application services or Western Digital issued devices;
- **Protected classification characteristics under California or federal law ("Protected Classes")** or characteristics protected under California and federal laws, such as your race, ethnicity, national origin, gender, gender identity/expression, sexual orientation, disability (including disability access and special related needs), immigration status, and military or veteran status where relevant;
- **Sensory data**, such as audio, electronic, visual, thermal, olfactory, or similar information, such as ID verification photographs;
- **Internet or other similar electronic network information** (in case of online job application), such as your IP address, log files, login information, information relating to your usage and activities on Western Digital's websites and information collected from cookies. Please refer to our Cookie Statement available on Western Digital's websites for more information on how we use cookies and other similar technologies, including how to exercise your rights to opt out of cookies; and
- Any other relevant personal information for assessing your professional skills in view of the job position you are applying for.

You may also voluntarily submit and attach documents for Western Digital to consider.

Some of the personal information collected by Western Digital is classified as "Sensitive Personal Information" or belongs to special categories of data, such as:

- Social security number, driver's license or government issued identification number;
- Certain protected classification characteristics such as your race, ethnicity, sexual orientation, health, and/or religion, only where required by applicable local law;
- The contents of your email or other electronic communications from your Western Digital email accounts or issued devices;
- Precise geolocation;
- Immigration status, only where required by applicable local laws;
- Disability access and special needs, where strictly necessary and permitted by applicable local law;
- Information from background checks, criminal convictions, only when required by applicable local law.

The provision of certain personal information may be necessary or optional. Mandatory data will be marked as such at the moment of collection of your personal information. If you refuse to provide mandatory data, you will not be able to submit a profile for a position.

WESTERN DIGITAL APPLICANT PRIVACY NOTICE

The Nature of Western Digital’s Processing Activities

Western Digital processes your personal information in compliance with applicable data protection laws and where there is a legitimate purpose for doing so.

To consider your application for employment, Western Digital processes your personal information for the following purposes:

Processing activity	Legal Basis	Data Retention period
<p>Recruit and selection of employees, which includes the acceptance of applications, the vetting of candidates, the management of interviews, deciding to whom we will offer a job, maintaining records related to recruitment, right to work verifications, regulatory purposes, such diversity requirements (where required under applicable local laws).</p>	<p>Where necessary to take steps to enter into the employment contract with the employee</p>	<p>Applicant files are maintained for 3 years after the close of the requisition, unless otherwise required by applicable local law where you work</p> <p>Work authorization records are maintained for 3 years after termination of employment, unless otherwise required by applicable local law where you work</p>
<p>Verification and source checking (only if authorized or required by applicable local law), which includes verifying the information provided to us in connection with applications, speaking to references, conducting background checks (when applicable).</p>	<p>When necessary to take steps prior to entering into a contract with the applicant</p>	<p>References and background checks are maintained for 6 years after creation, unless otherwise required by applicable local law where you work</p>
<p>Communicating with applicants, which includes maintaining contact information, and communicating with applicants.</p>	<p>Where necessary to take steps to enter into the employment contract with the applicant</p>	<p>Emails are maintained for 1 year, unless stored in an employee file, in which case they are stored for 7 years, unless otherwise required by applicable local law where you work</p>
<p>Updating the talent pool of Western Digital, which includes incorporating applicants in Western Digital talent pool in order to inform them about new professional opportunities within the Western Digital Group.</p>	<p>To fulfill Western Digital’s legitimate interest after taking into account the purpose and need of processing, and balancing the interests of Western Digital with the rights of the applicant</p>	<p>Applicant files are maintained for 3 years after the close of the requisition, unless otherwise required by applicable local law where you work</p>
<p>Internal process and improvement, which includes assessing and improving the performance and success of our</p>	<p>To fulfil Western Digital’s legitimate interest in improving its recruiting and hiring process</p>	<p>Applicant files are maintained for 3 years after the close of the requisition, unless otherwise</p>

WESTERN DIGITAL APPLICANT PRIVACY NOTICE

Processing activity	Legal Basis	Data Retention period
recruiting and hiring process, analysing best recruitment practices, making Western Digital a great place to work.		required by applicable local law where you work
Compliance with local laws, including equal opportunity laws , which includes diversity information if authorized or required by applicable local law. Note: When applicable, this may require Western Digital to process sensitive personal information about applicants, including their race, ethnicity, gender, or health information.	To comply with legal obligations to which Western Digital is subject as employer	Regulatory reporting is maintained for current year of report plus 6 years, unless otherwise required by applicable local law where you work Applicant files are maintained for 3 years after the close of the requisition, unless otherwise required by applicable local law where you work
Responding to accommodation requests , which includes assessing requests to accommodate applicants during the recruitment process, as well as post-hiring accommodations, where applicable. Note: Where authorized or required by applicable local law, this may require Western Digital to process sensitive personal information about applicants, including health information.	To comply with legal obligations to which Western Digital is subject as employer	Employee personnel files are maintained for up to 6 years after the termination of employment, unless otherwise required by applicable local law where you work Applicant files are maintained for 3 years after the close of the requisition, unless otherwise required by applicable local law where you work
Enforcing Western Digital's legal rights , which includes using personal information in connection with pre-litigation or litigation filed by or against Western Digital, reporting potential violations of the applicable local law with law enforcement agencies, responding to any request by law enforcement or government agencies, and responding to court orders, subpoenas, or discovery requests, whether or not these requests were made within or outside your country.	To fulfil Western Digital's legitimate interest in defending its rights and interests	Legal records are maintained for 10 years after the resolution of the matter, unless otherwise required by applicable local law where you work Applicant files are maintained for 3 years after the close of the requisition, unless otherwise required by applicable local law where you work

WESTERN DIGITAL APPLICANT PRIVACY NOTICE

Western Digital will process your personal information only for one or more of the purposes outlined above, for purposes sent to Western Digital employees in a separate notice, or in other ways that applicable local law may permit.

Automated Sorting of Applicants

In certain jurisdictions, Western Digital may use data analytics and algorithms to help us to review the large quantities of candidates and application data that we receive. These algorithms help us prioritize the application review process and sort candidates based on professional characteristics that suggest strengths and capabilities necessary to perform the relevant role.

These analytical tools do not characterize an automated individual decision-making to the extent they do not determine who is and who is not given offers of employment based solely on automated processing. Rather, Western Digital considers the results in combination with other information about the applicant, and each candidate's assessment is based on human judgment. We evaluate each individual candidate on their own merits.

Who Has Access to Your Personal Information

Your personal information can only be accessed by or disclosed to Western Digital employees who have a need-to-know, and the information they have access to is limited to the personal information that they need to perform their job. Specifically, the following employees within Western Digital will have access to your personal information:

- Human Resources team members;
- Those responsible about making decisions about your application for employment, such as Talent Acquisition and those with whom you have interviewed;
- Hiring managers;
- Security personnel to the extent you have had to enter a Western Digital business location;
- Professional advisors, such as lawyers; and
- Other employees who have a legitimate business reason for processing your personal information.

Your personal information may also be shared with other corporate entities associated with Western Digital in order to globally manage the human resources within Western Digital Group.

Western Digital will not provide your personal information to a third party unless that third party undertakes to: implement and maintain appropriate security measures; comply with applicable local laws; only use your personal information where required and for the purposes for which your personal information was provided by Western Digital; and guarantee at least the same levels of protection for your personal information as required by Western Digital. We may also share your information with former employers to obtain a reference or confirm employment history.

Western Digital stores your personal information in various business applications and may disclose your personal information to service providers that assist Western Digital in providing its services. Your personal information may be accessed and stored by such service providers for administrative, technical and operational purposes.

Western Digital may provide your personal information to local regulators in order to comply with legal obligations. Your personal information may be provided to law enforcement agencies or to law firms in connection with any legal proceedings or in response to subpoenas or similar requests. Similarly, Western Digital may be under an obligation to disclose your personal information to regulators, courts, the police or local authorities, or in the course of litigation. It may not be possible to notify you in advance about the details of such disclosures. In such cases, Western Digital will use all reasonable efforts to disclose the minimum personal information necessary.

WESTERN DIGITAL APPLICANT PRIVACY NOTICE

Finally, Western Digital may also provide your personal information to successor businesses in the event of a corporate business transaction, such as a merger, acquisition, joint venture, or financing or sale of company assets.

Where Western Digital Transfers Your Personal Information (International Transfers)

From time to time, Western Digital transfers your personal information outside of your home country to its subsidiaries and affiliates, as well as third parties (e.g., service providers) in the US and elsewhere where there is a business need to do so and for the purposes described above.

Western Digital also transfers your personal information to third parties in Europe and around the world where required by law (e.g., to tax authorities), to protect its legal rights (e.g., to defend litigation, legal advice or audit requirements) or in an emergency (e.g., in a workplace accident where an employee's health or security is at risk).

Where Western Digital transfers your personal information to a country that may not have the same level of privacy protection as your home country Western Digital will ensure that the transfer is covered by appropriate safeguards (for example, by entering into standard contractual clauses as adopted by the European Commission or the UK Data Protection Authority), and will implement measures to act in accordance with applicable data protection laws. If you want more information about the potential third countries where your personal information is transferred and obtain a copy of the associated safeguards, you can reach out Western Digital's Data Protection Officer (DPO) by email at privacy@WesternDigital.com.

Western Digital Security Measures

Western Digital is committed to taking appropriate technical, physical and organizational measures to protect employee personal information against the following: unauthorized or accidental destruction; alteration or disclosure; accidental loss; unauthorized access; misuse; unlawful collection/use; and damage.

Your Rights and How You Exercise Them

Depending on the laws of your jurisdiction, and including the residents of California, you may have certain rights with respect to your personal information:

Your rights	Scope
Right to access	You can request that we disclose to you the following to the extent applicable to you: (i) the categories of personal information that we have collected about you; (ii) the categories of sources from which we have collected personal information about you; (iii) the purpose for collecting, sharing, or selling your personal information (if applicable); (iv) the categories of personal information that we have sold or shared about you and the categories of third parties to whom the personal information was disclosed (if applicable); (v) the categories of personal information that we have disclosed about you and the categories of third parties to whom the personal information was disclosed; and (vi) the specific pieces of personal information that we have collected about you. If you request to access information related to our use of ADMT specific to you, unless a legal exception applies, we will disclose to you: (i) the specific purpose for which we use ADMT to make a significant decision about you; (ii) information about the

WESTERN DIGITAL APPLICANT PRIVACY NOTICE

	ADMT's logic that explains how the ADMT processed your personal information to generate an output about you; and (iii) the ADMT's outcome for you, including how we used the ADMT's output to make a significant decision about you and whether we may use the output to make future significant decisions about you.
Right to rectification/correction	You have the right to correct or request the rectification of your personal information if your personal information is obsolete, inaccurate or incomplete.
Right to delete	Under certain circumstances, you have the right to request the deletion of your personal information.
Right to restriction of processing	Under certain circumstances, you have the right to request the restriction of the processing.
Right to portability	Under certain circumstances, you have the right to request a copy of your personal information in a structured, commonly used and machine-readable format and also can request their transmission to another data controller where technically feasible.
Right to object	Under certain circumstances, you have the right to object to our processing of your personal information.
Right to withdraw your consent	You have the right to withdraw your consent when it has been obtained.
Right to opt out of ADMT or other automated individual decision-making technologies (California, Colorado and New York City residents only)	You have the right not to be subject to a decision based solely on ADMT (as defined by the CCPA) or other automated processing technologies including profiling, which produces legal effects on you or similarly significantly affects you unless a legal exception applies.

Depending on your country of residence, you may have additional local rights with respect to our processing of your personal information. For example, if you are based in France, you can [define either](#) general or specific guidelines regarding your personal information in the event of your death (e.g. their deletion or transmission to any person of your choice).

You also have the right to lodge a complaint before your national data protection authority. For those in Europe and the UK, please see the list and the contact of the data protection authorities [here](#). Western Digital does not prohibit applicants from lodging a complaint with the relevant government office if a Western Digital applicant has any concerns with the processing of their personal information. Please feel free to directly contact Western Digital before discussing with regulators, so that any issue may be resolved in cases of mistakes.

If you want to exercise your applicable rights, you may directly contact our Data Protection Officer (DPO) by email at privacy@wdc.com. You may also reach us at (855)-799-5529 or via our [webform](#) or write to us at a [location](#) nearest you via mail addressed to: ATTN: Legal Department - Privacy Statement Question.

WESTERN DIGITAL APPLICANT PRIVACY NOTICE

We will respond to your request in the timeframe required by applicable law (and in general within 30 days).

As required by law, and to protect the privacy and security of your personal information, we may request information from you to enable us to confirm your identity and right to access such information, as well as to search for and provide you with the personal information we maintain.

There are instances where applicable laws or regulatory requirements allow or require us to deny a request.

Authorized Agent: You may authorize an agent to submit a request on your behalf, so long as you provide the authorized agent written permission signed by you to make a request on your behalf, and your authorized agent additionally is able to verify their identity with us. If you are a resident of California and would like to designate an agent for purposes of making a request, your agent must register as such with the California Secretary of State and submit a copy of this registration along with your verified consumer request. Please have your authorized agent follow the instructions above to make a request and additionally mail your written declaration authorizing the agent to act on your behalf, certified by a notary public, to: Legal Department, 5601 Great Oaks Parkway, San Jose, California 95119 USA. If your authorized agent has power of attorney, it may not be necessary to perform these steps.

If you request to delete your data, this may remove your ability to access any Western Digital accounts. In addition, we may retain some personal information related to you if authorized or required by applicable laws, notably it may be necessary to keep some personal information in order to prevent fraud or future abuse.

We will not discriminate or retaliate against you for exercising any of your privacy rights identified in this Notice.

Changes To This Notice

We may update this Notice from time to time. When we make changes to this Notice, we will change the date at the beginning of this Notice. If we make material changes to this Notice, we will notify you by email to your registered email address, by prominent posting on our websites, or through other appropriate communication channels as required by applicable local law. All changes shall be effective from the date of publication unless otherwise provided in the notification.

Questions

To ask any questions related to this Notice or Western Digital applicant and recruitment privacy practices, or to exercise any legal rights that you have related to your personal information, please contact applicantprivacy@wdc.com.

You may also contact Human Resources with requests for access or regarding any complaints related to your personal information.