

Workday Recruitment Privacy Statement

Effective June 3, 2026



Recruitment Privacy Statement

Effective: June 3, 2026

[Prior Recruitment Privacy Statement](#)

Introduction and Statement Scope

Workday respects individual privacy rights. We are committed to handling your personal information fairly, responsibly, and in accordance with applicable local laws.

This Recruitment Privacy Statement explains how Workday collects, uses and protects your personal information in connection with our recruitment efforts for roles with the **Workday group**. This Privacy Statement also explains individual privacy rights. It applies to:

- **Prospective and Active Applicants and Candidates:** including those that apply directly for a Workday position or are referred to us, and those individuals that we identify in the market
- **All Role Types:** including full-time or part-time employment or internship opportunities.

Workday has offices all over the world and this is a global Privacy Statement. While our core principles remain consistent, how we process personal information can vary based on local laws, the recruiting locations or the role type.

Further transparency: Workday and authorized third parties may provide additional privacy notices to keep you informed about our recruitment related data processing. These notices can be provided at various touch points, such as when we collect the information, when we meet with you, or within the tools you interact with.

Workday's Role in Recruitment

Workday is a leading provider of enterprise cloud applications for finance and human resources. This means Workday customers, e.g. companies, schools, governments and other organizations use our software applications to manage their recruitment efforts, workforces, and finances.

- **If you applied for a role with a Workday company:** this Privacy Statement applies to you.
- **If you applied for a role with another company or Workday customer:** This Privacy Statement does not apply. As a cloud application services provider, Workday does not control or make recruiting decisions for customers using Workday applications.
- Workday cannot respond directly to a request where the personal information processed relates to another organization's recruitment, instead, please refer to the recruiting organizations' privacy statement for contact information.

Quick Links

We encourage you to read this Privacy Statement in full. If you're looking for specific information on our recruitment data practices, you can also easily jump to specific sections.

[What personal information do we collect and process?](#)

[Does Workday process sensitive personal information?](#)

[When is personal information required?](#)

[Will you contact me about future Workday roles and potential matches?](#)

[Does Workday share your personal information?](#)

[Does Workday use Artificial Intelligence \("AI"\) tools?](#)

[Can my personal information be used for recruitment research, training or development?](#)

[How long does Workday retain your personal information?](#)

[What are your privacy rights?](#)

[How does Workday protect your personal information?](#)



[Does Workday transfer your personal information internationally?](#)

[Certifications](#)

[Will Workday make changes to this privacy statement?](#)

[Want to contact us?](#)

[Additional region-specific disclosures](#)

What personal information do we collect and process?

Information you provided directly when you

Information will be collected directly from you when you:

- introduce yourself to Workday at an event or join the [Workday Talent Community](#) to be considered for potential future roles
- create a candidate account on our careers portal
- apply for a role at Workday
- meet us during Workday or associated events or interviews e.g. in person, or phone or during video meetings

Information obtained from other sources

As you move through the process, our recruiting teams and systems generate information about your application and candidacy.

We collect information from external sources outside of Workday, when considering applications or searching for talented personnel, in accordance with applicable law, including:



- **Professional careers platforms:** you can apply for a role at Workday using third-party applications and sites, such as LinkedIn and SeekOut. This connects your profile with Workday systems and our application process
- **Recruiting agencies, academic institutions, professional organizations, alumni and resume sharing platforms** and similar parties supporting job searches
- **Workday personnel** who recommend or refer you
- **Background checking and verification suppliers**
- **Referees** in response to reference requests
- **Public sources**, including any professional platforms you use and other relevant professional information available online, such as articles you may have written, research contributions or similar citations
- **Future group companies** that join the Workday global structure through a merger, acquisition or purchase of assets.

Table 1 summarizes the typical talent and recruitment purposes with examples of the personal information processed and the legal basis where applicable.

You can read more about the “legal bases” we rely on to process personal information in Tables 3 and 4

Table 1: Personal Information We Collect and Process

No.	Purpose	Examples of Personal information processed for this Purpose	Legal Basis for Processing
1	Providing access to our recruitment site, posting job specifications, and managing site security.	We process the following personal information for this purpose: • Recruitment site account information: registration details, residential address, email address, phone number and other contact information and site account passwords. • Information about use of our recruitment site: we may deploy tools and cookie technologies to assess website	Legitimate interests Consent

		usage. This includes information about how many individuals are visiting job posts, how long they are staying on the sites, which pages are most popular, devices and IP addresses.	
2	Identifying and shortlisting prospects and job applicants.	We process the following personal information for this purpose: • Information concerning your job application(s): application letters, resumes/CVs, including: skills, education and academic records, employment experience descriptions, roles and prior job titles, years of experience in a role or industry, languages, reasons for moving, notice periods, professional qualifications and certifications, right to work and security clearances. • Information that identifies you: including your full and known names, gender, date of birth, age, your generation, national identifiers, government	Legitimate interests Contract and pre contractual necessities Explicit consent

		identification numbers, photographs, codes and documentation, citizenship, nationality and passport information. • Information connected with your current location: residency information, distances from offices and work preference types, including remote, onsite or flex work options. • Information from online research: professional profiles online, publications, interviews, blogs, registrations, certifications and citations. • Verifying contact information: email, address or phone numbers, in connection with out-reach to prospective individuals who have not registered a careers account with us. • Information on your interests: details of any memberships or professional and private interests, hobbies (which may include information revealing <u>“Sensitive Personal Information”</u>)	
--	--	--	--

		described below).	
3	Facilitating our recruitment processes and managing in-person and online meetings and assessments.	We process the following personal information for these purposes: • Information about your schedule: meeting availability or geographic location and mobility that you provide to your talent acquisition contact within your application information or via automated scheduling invites, virtual assistant, or chatbot technology functions and communications tools. • Information about the roles you are interested in, future jobs, and professional goals • Information about your required adjustments to working arrangements: To the extent required or permitted by local law, we process information concerning health and any disabilities in connection with any adjustments or accommodations to interview and	Legitimate interests Consent

		working arrangements you require (which may include information revealing <u>“Sensitive Personal Information”</u> described below). • Information about your compensation expectations: future package and benefits aspirations. • Information about your travel expenses: current and future data on your expenses and banking details so that Workday can reimburse approved travel expenses. • Information from meetings, calls and presentations: notes or summaries of your responses including audio, voice data, or images where we record the meeting or presentation. • Assessment information: the results of a candidate assessment or certified skills test with Workday or a third-party provider if we ask you to complete a role-specific, job related assessment during the	
--	--	---	--

		recruitment process. • Information about your referees and reference providers: their name and contact details, employer, job role, relationship to you and their views about your previous roles and suitability. • Video: images if you attend an interview or assessment at a Workday office, including images captured by video surveillance cameras used for safety and crime prevention purposes. For more information, see our Video Surveillance Privacy Statement.	
4	Making a hiring decision for current or future employment opportunities.	We process the following personal information for this purpose: • Information relating to our assessment of your application: including our interview and meeting notes and summaries, and confidential interviewer opinions, your references, role-relevant public information, as well as records of our decision-making process.	Legitimate interests

5	Verifying your information and carrying out necessary background checks. • Once you have signed a job offer or agreement, Workday or our independent supplier will reach out to you to begin the background check process. • Designated hiring service team members are informed if a check meets or does not meet company standards, but Workday does not hold the underlying information verified. If there is a discrepancy, we will notify you of next steps.	We or our approved service providers process the following personal information for this purpose in connection with the relevant activities: • Verifying the accuracy of the information you or referees provide: evidence of prior employment history, roles, locations and dates, education and professional qualifications or registrations. • Background checks: To the extent required or permitted by local law, verifying your identity, security clearances and other background or consumer reports applicable to the role, Workday or customer projects, assignments or secondments (which may include information revealing <u>“Sensitive Personal Information”</u> described below). • Information about your right to work: To the extent required or permitted by local law, we process personal information to verify your eligibility to work	Consent Explicit Consent Legal obligation
---	---	---	--

		in a given location, assisting you with obtaining a migrant visa or work permits, details of your work permit applications, permit status, expiration dates, permitted work categories, visas and visa numbers, passports, citizenship or nationality, ID card information including numbers, photographs, social or tax codes.	
6	Promoting, monitoring, and reporting of diversity and equal opportunities	We process the following personal information for this purpose: Information necessary to monitor Workday's non-discrimination and inclusivity obligations, or to meet local regulatory reporting requirements: To the extent required or permitted by local law, information on your nationality, racial and ethnic origin, gender including gender identity, sexual orientation, religion, disability and age which may be aggregated (see more on this below). This may	Legal Obligation Consent Explicit Consent

		include information revealing <u>"Sensitive Personal Information"</u> described below.	
7	Defending Workday against potential complaints, enquiries and responding to legal requests.	We process the following personal information for this purpose: • Complaint and legal response information: your own and third-party views about you or the concern raised, comments regarding suitability, and other responses in connection with your application and our handling of this. The specific information processed depends on the nature of the complaint, inquiry, or request and who raises it.	Legal obligation Legal claims Legitimate interests
8	Improving Workday's recruitment processes and services.	We process the following personal information for this purpose: • Feedback information: any information on the Workday recruitment process provided to Workday talent acquisition or other Workday personnel, Workday staff or via voluntary surveys initiated by Workday. • See also "<u>Can my personal</u>	Legitimate interests

		information be used for recruitment research, training, testing or development?"	
9	Contacting you about future Workday opportunities and news.	We process the following personal information for this purpose: • Talent Community and Unsuccessful Candidate Database Information: your contact details, contact preferences, roles you mention you are interested in, how we were introduced to you, (e.g. whether via an event, introduction, third party careers website, etc.), your profile suitability for specific job requisitions and any prior applications See more on the section: "Will you contact me about future Workday roles and potential matches?" and "Does Workday use AI tools to process my job applications to support the recruitment process?" below.	Legitimate Interests Consent

Information collected automatically

When you visit the Workday Recruitment site, we use cookies, tracking pixels, and scripts. For more information about the technologies we use, why we use them, and how you can control these technologies, please review the [Workday Recruitment Site Cookie Notice](#).



Does Workday process sensitive personal information?

Yes, but only if we have legitimate business or legal reasons.

We understand that certain personal information requires greater protection. The meaning of “sensitive” or “special category” personal information differs globally, but typically includes information about your racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, biometric data, data

concerning health, sexual orientation, and criminal history. In some jurisdictions, it can also include the contents of your communications where Workday is not an intended recipient, or your precise geolocation.

As a rule, we do not process sensitive personal information about you unless required or permitted under your local laws. In certain situations, we may need to collect, or request sensitive personal information on a voluntary disclosure basis, e.g.

- **Fairness for Everyone:** information about your racial or ethnic origin, gender, gender identity, sexual orientation, and disabilities collected to assess fairness and non-discrimination, and to create and cultivate an inclusive work environment, including where required:
 - to comply with equal employment opportunity reporting obligations or goals, and anti-discrimination laws and applicable authority reporting obligations.
 - to strengthen [Workday Value, Inclusion, and Belonging for Everyone](#) practices with your explicit consent, where required by applicable laws.
- **Supporting You:** Information about your physical or mental condition to provide work-related accommodations, such as during fitness to work dialogue. You may also provide sensitive information to health and insurance benefits providers that Workday arranges for you if you are successful in your application

If we need to collect sensitive personal information, we will do so in a way that is lawful, tell you and explain how we will use it.

Workday is proud to be an equal opportunity workplace. Workday does not use sensitive personal information to make recruitment or employment decisions. As a general rule, you can decline to provide sensitive personal information if you prefer not to say. There is no negative impact on any application if you prefer not to say.

When is personal information required?

Workday will inform you if there's a legal, business or recruitment requirement to provide personal information. Generally, we'll only ask for what is necessary and proportionate to consider you for a role and the relevant recruiting purpose. If you're unable to provide the information required, we'll explain if there might be any consequences or delays to your applications.

When we ask for your consent to collect or use your personal information by Workday or a third party, you're not obliged to give consent - you can choose freely whether you wish to consent to that specific collection or use.

Will you contact me about future Workday roles and potential matches?



Yes.

- **Talent Community:** If you are curious about Workday but there is not a current job opening you wish to apply for, you can become a member of the [Workday Talent Community](#).
- **Staying in Touch:** If your if your initial job application is not successful we'll add your information to our internal Candidate Database and may reach out to you about future roles. You can advise your talent acquisition contact if you'd prefer not to be added.

During future recruitment initiatives, Workday may:

- Send you information about Workday news and career events
- assess if there are matches where your profile might be a fit for an upcoming role and may invite you to apply.

Workday Talent acquisition assesses your resume/CV, qualifications and experience when identifying and shortlisting potential candidates based on prior exchanges with you and may use Workday's AI tools. You can provide a new version of your resume/CV at a later point and update your contact preferences at any time.

See: "[Does Workday use AI tools to process my job application to support the recruitment process?](#)" and "[What are your privacy rights?](#)"



We will keep the information for future job match purposes for a reasonable period after your application based on local laws and guidance.

Compliance: Keep in mind, if your initial application is unsuccessful, we need to retain information to respond to queries and assess compliance with local laws for a period, but you can still ask to be removed from future role consideration, job invitations and Workday news. See: [“How long does Workday retain your personal information?”](#).

If you accept a role at Workday, the information we collect during recruitment becomes part of your personnel file and Workday profile. We will provide our Employment Privacy Statement during your onboarding process to explain how Workmate personal information is managed.

Does Workday share your personal information?

There are a number of situations where we may need to share your personal information with others in line with the recruitment and business purposes outlined in Table 1. Workday takes care to disclose personal information to only those recipients who require access to perform legitimate tasks and duties.

Internally within Workday: Workday personnel authorized to access or discuss recruitment personal information, including talent acquisition, hiring, technology and analytics teams, must comply with confidentiality, privacy and security policy requirements. Members of the Workday group around the world support our recruiting efforts.

External to Workday: Your personal information is shared with third parties where necessary and on a “need to know” basis. This is usually to meet a legal requirement, connected to a contracted service or other recruiting or business interests that do not outweigh your individual rights.

Table 2: Who we may need to share your information with:

Recipients, external parties and sharing scenarios	Reasons for sharing
Workday-contracted third-party suppliers and service providers: This may include recruiter systems and technology, software providers, including virtual assistants and chatbots, recruitment and search agencies, testing or assessment institutions, survey tool providers, payment processors, travel management, our background checks providers, and benefits providers.	These parties support Workday with e.g. training and assessments, payment processing, travel and safety, software and technology interactions.
Legal and Regulatory Bodies: Courts, tribunals, regulators, public authorities, and professional advisers (including immigration specialists, tax advisers, accountants and lawyers).	Workday may need to share to comply with our legal and regulatory obligations, inquiries or matters, including to respond to a complaint, court order, audit, warrant, subpoena, administrative, regulatory or judicial process, request or incident.
Other Third parties where necessary:	

- | | |
|--|--|
| <ul style="list-style-type: none">• to establish, exercise or defend against potential, threatened, or actual litigation.• when we have a good faith belief that disclosure is necessary to protect your safety, the safety of others, or compliance with local standards applicable to Workday.• in connection with a business transition or restructure, such as a merger, acquisition by another company, or sale of all or a portion of Workday's assets.• where you've consented or instructed Workday to share your personal information or where disclosure is reasonable. | |
|--|--|

- **Third-party suppliers and service providers.** When we engage third party suppliers to process personal information on Workday's behalf, we implement appropriate measures to ensure they handle information in a way that aligns with this Privacy Statement and applicable law and to maintain the security and confidentiality of the information. This is in addition to any legal, privacy and security duties the third party has in connection with their services under applicable law.

Third-party recipients also have their own privacy statements outlining their data processing approach, that you may wish to consult where the third party has their own business purposes or if you have a direct relationship with them.

Does Workday use Artificial Intelligence (“AI”) tools?

Yes. We use responsible AI tools across various stages of the recruiting process, e.g. to help review applications, schedule interviews, and capture meeting notes. AI supports our processing of personal information for the recruitment and business purposes described in **Table 1**. Workday is committed to using tried, tested and trusted AI tools that both empower and support the human judgment and the valuable experience of our talent acquisition team members. We believe AI can significantly enhance the recruitment experience for our prospective workmates. We may also provide more information regarding these AI tools at the specific stages of your candidate journey.

Workday implements robust risk management practices to test our AI tools for fairness and to mitigate bias and similar risks. We seek assurances from third parties that may provide AI tools before any deployment, alongside due diligence reviews.

Does Workday use AI tools to process job applications to support its recruitment process? Yes. We receive very large volumes of applications and candidates, and to process these we use AI tools that help our recruiters identify and evaluate how closely candidate applications and resumes/CVs align with a given job requisition. The AI-powered tooling helps to improve consistency, accuracy and speed in the recruitment process and reduce the potential for human bias or errors.

How does it work? The AI tooling extracts personal information from within candidate applications and resumes/CVs that are *relevant* to the open role such as information you have disclosed about your skills, experience, location, and education as applicable. The tools then work out how closely this personal information matches the requirements of the role available and assigns a suggested grade reflecting how close the match is, for example: “candidate exceeds”, “meets” or “does not meet some or all the basic qualifications”.

The Workday talent acquisition team uses these suggested AI generated grades to help shortlist and prioritize applications in the recruitment process. Our talent acquisition team is trained in the responsible use of AI recruitment tools and as a general rule the grades are one of several factors they consider throughout the candidate consideration process for those minimally qualified for the role, in conjunction with screening interviews and hiring manager interviews. Workday hiring managers and prospective teammates in the recruiting department are involved in ultimate hiring decisions across all stages of the hiring process.

In some recruitment exercises, for example, where we have particularly high volumes of applicants, it is not possible for every CV/resume or application to be reviewed by a member of the talent acquisition team during initial sifting stages, and so your application may not be successful if an open role is filled while you are still in the recruitment process and/or you do not meet the minimum job requirements.

We will use such AI recruitment tools consistent with the requirements of applicable privacy laws. For more information, see: [“What are your privacy rights?”](#) below.



Can my personal information be used for recruitment research, training, testing or development?

Yes. We may use the personal information our candidates submit for recruitment research, training, testing and development, including:

- **Business research and reporting:** Workday may produce or receive summary reports for Workday's talent acquisition teams and leaders to understand overall recruitment metrics, including volumes, geographies or candidate pool inclusivity and progression trends. Recruiting research and reports help inform future recruitment strategies and third-party learning opportunities.
- **Product development:** Workday's own product technology can be developed using applicant and candidate data leveraged in Workday recruitment practices. AI models (that support the functioning of Workday AI products) may be improved and trained by learning from patterns manifest in Workday's own recruitment practices, for example, recruiters for "sales roles" tend to advance candidates with "negotiation experience" therefore future iterations of Workday's AI models may learn to place greater weight on "negotiation experience" for those select roles without impacting you personally - such improvements could help future applicants and candidates. These enhancements also support Workday and third parties including customers who later use Workday's cloud application services for future recruitment exercises.
- **Internal testing:** Workday may conduct assessments to support its responsible AI commitments to manage risks related to fairness, non-discrimination, inclusivity and efficacy.

Does Workday apply privacy enhancing techniques?

Yes to protect privacy, we aim to implement privacy enhancing and security safeguards to responsibly use certain information within wider data sets to protect individual privacy. Specifically, Workday and authorized third parties may use de-identification, pseudonymization, and/or aggregation techniques, which are designed to mitigate and reduce individual privacy risk impacts when possible. . This can occur, for responsible security and when Workday runs, research, data science, analytics, reporting, learning, improvement and product development purposes. or responsible security, research, analytics, reporting, product development purposes.

Workday's use of this data for responsible product development, reporting and testing supports Workday's legitimate interests in innovation and improvement. Workday is required to work with quality and representative candidate datasets to train, test and develop Workday's AI technology.

Please note that Workday does not share or license personal information provided during your applications to Workday, including identifiable job applications, resume/CV information, suggested grades or reports with other businesses for their own recruitment or other purposes.

How long does Workday retain your personal information?

Workday securely stores and retains your personal information for the time periods needed to fulfill legitimate business purposes, including those described in this Privacy Statement and in accordance with applicable local laws. In summary, we keep personal information:



- Following the completion of a recruitment process and hiring decision so that we can consider and respond to potential enquiries, complaints, legal or compliance matters involving Workday's recruitment operations
- To keep you informed of future vacancies if you wish and maintain accurate records of your contact preferences.

You can update your preferences regarding future contact at any time, but please be aware that we'll need to retain other information if we have lawful bases and purposes at the time of the request.

We have processes in place to delete recruitment information between six months and four years following an unsuccessful application. The period differs based on local laws and guidance in the recruiting location. To determine the appropriate retention period for personal information within our records, we consider many factors relevant to the Workday business and your recruitment, including:

- our legal and regulatory obligations or any available guidance
- claims risk and limitation periods
- prevailing legitimate business needs
- the amount, nature, and sensitivity of the personal information
- the potential risk of harm from unauthorized use or disclosure of your personal information considering our technical security controls
- if we can achieve any prevailing purposes through other means.

What are your privacy rights?

You may have specific legal rights over the personal information we hold about you. These rights vary depending on the recruiting and role locations but generally can include the ability to:

- **Access, Correct and Delete:** you can request to see a copy of the personal information processed by us, correct inaccurate personal information and ask for it to be deleted.
- **Object to Workday's Processing:** You can object to the processing of your information if we are relying on our legitimate interests as the legal basis.
- **Restrict Processing:** You can ask us to temporarily limit the processing of your information.
- **Request Portability:** If we are processing your personal information with your consent or under a contract, you can request a copy of it in a structured, commonly used and machine-readable format so you can easily transfer it.
- **Withdraw your consent at any time:** If you gave us consent to process your personal information, you can withdraw it later. This won't affect any processing we did before you withdrew the consent, nor will it impact processing we conduct based on another legal basis.
- **Not to be subject to a solely automated decision (including profiling) which produces legal or similarly significant effects.** Under applicable privacy laws, we can only use solely automated tools that produce legal or significant effects within our recruitment processes in certain circumstances and with specific safeguards. For example, if we have your consent to do so, it is necessary to enter into or perform a contract with you, or we are authorised by law. In such cases, you can contact our talent acquisition team and seek a human review.
- **Lodge a complaint and seek redress.** If you have information handling concerns, or you feel there has been a violation of local privacy laws you can:
 - Lodge a complaint with the Workday recruiting company
 - Lodge a complaint with a local data protection supervisory authority

How does Workday handle requests and complaints?

Workday will not discriminate against you for exercising your privacy rights. We'll explain how any of the rights operate in your situation, e.g.

- If the right differs in your location or because of the legal basis for the processing activity
- If Workday has prevailing processing needs and what they are
- How the rights of other individuals or parties interact with your specific request.

How can I raise a query or exercise my privacy rights?

You, or someone authorized to act for you, can exercise your privacy rights by submitting a request via our online form. You can also use the details in ["Want to Contact Us?"](#). We may need to ask for verification in some cases.

If you can provide details of your concern, this can assist Workday expediting the response. In any event, we will work to process the request and respond within a reasonable timeframe under applicable law. We aim to keep you updated. We usually respond within one month of your request, but we can extend in complex cases.

If we cannot resolve your complaint, you can contact the data protection supervisory authority or court in your usual place of residence or work, or at the ["Controller's"](#) registered office.

The ["Additional region-specific disclosures"](#) section provides more information about local supervisory authorities. You can also request the confirmation of the competent data protection supervisory authority using the details in the ["Contact Us"](#) section.

If we have not resolved your privacy or data use concern satisfactorily, you can also contact our third-party dispute resolution provider (free of charge) at this link: <https://feedback-form.truste.com/watchdog/request>.

APEC Cross-Border Privacy Rules System

The Workday privacy practices described in this Privacy Statement, comply with the APEC Cross-Border Privacy Rules System ("CBPR"). The APEC CBPR provides a framework for organizations to ensure protection of personal information transferred among participating APEC economies. More information about the APEC framework can be found [here](#).

How does Workday protect your personal information?

We use a combination of security arrangements to protect your personal information. This includes implementing technical, organizational and contractual measures to protect the personal information from accidental loss, destruction, or other incidents and risks.

We also require suppliers to implement appropriate security measures based on the risks associated with their services and the relevant personal information they handle. These measures are in addition to any legal, privacy and security duties they already have under applicable law.



Please note security of information transmitted through the internet can never be guaranteed. You are responsible for maintaining the security of your password or other form of authentication involved in accessing password-protected or secured areas of any Workday recruitment web page or process. Access to and use of password-protected and/or secure areas of any Workday recruitment web pages or processes are restricted to authorized users only.

Does Workday transfer your personal information internationally?

Yes. Workday is headquartered in the U.S. and operates as a global business. We transfer, store, access and process your personal information in various international locations, including countries:

- where you are applying or being considered for a role
- outside your jurisdiction
- where [Workday](#) or Workday-contracted third-party suppliers, customers or relevant third-party recipients have operations.

Certifications

Workday adheres to the principles of the EU-U.S. Data Privacy Framework, the UK Extension to the EU-U.S. Data Privacy Framework, and the Swiss-U.S. Data Privacy Framework (collectively the “DPF”) maintained by the U.S. Department of Commerce. Workday relies on the DPF as a legal basis for transfers of personal information to the U.S. To learn more, visit our Data Privacy Framework Notice [here](#).

We also implement additional safeguards to ensure adequate cross border data protection. For more details, see the “[Transferring personal information internationally](#)” section.



Will Workday make changes to this Privacy Statement?

We may update this Privacy Statement occasionally to reflect changes in our legal and regulatory duties, as well as recruitment, business and technology practices.

How we'll notify you: We will take appropriate measures to inform you about significant changes.

Accessing the current version: You can see when this Privacy Statement was last updated by checking the “last updated” date displayed at the top of this Privacy Statement.

Want to contact us?

Who is the Data Controller?

The Workday group company that is recruiting is a data controller with responsibilities to you. You can find a list of Workday affiliates and their further contact details [here](#) (the “**Local Workday Affiliate**”). In some locations, the Local Workday Affiliate company shares data protection responsibilities with additional Workday group members and headquarters that drive recruitment activities and strategies. You can read more on how Workday ensures data protection within the group and [“joint controllers”](#) below.

How can I raise Privacy questions?

Webform: If you have any questions about this Privacy Statement, our recruitment privacy practices, or wish to exercise your privacy rights, please submit your request through our [web form](#).

Mail:

If you are applying to a role located in the EEA, UK or Switzerland, you can mail:

Workday Limited
Attn.: Privacy
Kings Building, May Lane
Dublin 7
reland

If you are applying to a role located anywhere else, you can mail:

Workday, Inc.
Attn.: Privacy
6110 Stoneridge Mall Road
Pleasanton, CA 94588
USA

You can contact the Workday affiliate in the country in which you applied for a role or responded to a recruitment search process with any questions about your personal information. For a list of Workday affiliates and their contact details, see [here](#).

No matter where you are based, or how you contact us, we are committed to complying with

local privacy laws and protecting your personal information.

Additional region-specific disclosures

California

If you're located in California, please note the following additional disclosures:

Workday does not “sell” to third parties, or “share” with third parties for targeted advertising purposes, the personal information that it collects or processes as part of the recruitment, employment, or personnel management process or any related processes (including as those terms are defined under the California Privacy Rights Act).

For California residents, if you are submitting a request to access, please specify if you would like to access personal information categories or specific pieces of personal information. In addition to many of the rights described above, California residents have the right to opt out of a business's sale of your personal information or sharing of your personal information to third parties for targeted advertising. **Workday does not sell your personal information or share your personal information with third parties for targeted advertising.** Workday also does not use your sensitive personal information for any purpose other than to operate our business, for legitimate recruitment-related purposes, or where otherwise permitted by, or necessary to comply with, applicable laws, and therefore does not provide a right to limit the use of sensitive personal information.



When you submit a request, we will first acknowledge receipt of your request within 10 business days after receipt of your request. We will provide a substantive response to your request within 45 calendar days after its

receipt. If we require more time (up to 90 days or the permitted time frame), we will inform you of the reason and extension period in writing.

Only you or an authorized agent (as described below) may make a verifiable consumer request related to your personal information.

- **How to Authorize an Agent.** You may designate an authorized agent to submit your verifiable consumer request on your behalf only if the authorized agent has your written permission to do so and you have taken steps to verify your identity directly with us.
- **How We Verify Your Request.** To respond to your request, we must verify your identity and/or the authority of your authorized agent. We will only use the personal information provided to us in that context to verify your identity or the authority of your authorized agent to make the request. Making a verifiable consumer request does not require you to create an account with us. To allow us to verify your request, we may require that you provide at least two pieces of personal information that we already have in our possession, if we cannot already verify you. We will verify your consumer request by comparing the information you provide to information already in our possession, and take additional steps to minimize the risk of fraud.

European Economic Area, United Kingdom and Switzerland

If you're located in the EEA, UK and Switzerland, please note the following additional disclosures:

Joint data controllers

Workday Limited is the data controller primarily responsible for protecting your personal information and shares responsibility for protecting your personal information with the European Local Workday Affiliate that you applied to, or that has contacted you about a **role**. Workday Limited and the Local Workday Affiliate are joint data controllers.

We encourage you to contact Workday Limited with any questions you have about your personal information, although you can also contact your Local Workday Affiliate if you prefer. As between Workday Limited and your Local Workday Affiliate, Workday Limited is primarily responsible for:

- Preparing and providing you with this Privacy Statement
- Fulfilling any requests you make to exercise your privacy rights
- Determining the lawful bases for processing of your personal information
- Ensuring appropriate technical and organizational security measures are implemented to protect your personal information
- Reporting any personal data breaches that may occur in accordance with applicable privacy laws
- Conducting data protection impact assessments where required
- Engaging a third party supplier or data processor
- Ensuring appropriate safeguards have been implemented in respect of any international transfers of



personal information

Workday Limited is based in Ireland and is Workday's main establishment and European headquarters. Workday Limited is regulated by the Irish Data Protection Commissioner, whose contact details are available [here](#).

Workday Limited and your Local Workday Affiliate will cooperate as necessary to ensure the proper fulfillment of the responsibilities described above, in addition to any other requirements that apply under this Privacy Statement and privacy laws. Both will ensure compliance with the data protection principles at all times.

Contact details for Workday Limited and your Local Workday Affiliate are provided under the "[Want to Contact Us?](#)" section above.

Lodging a complaint

You may lodge a complaint with a data protection authority such as the supervisory authority of your usual place of residence. A full list of EEA data protection authorities is available [here](#). Contact details for the Irish Data Protection Commissioner are available [here](#). In the UK, the data protection authority is the [Information Commissioner's Office](#) and in Switzerland the [Federal Data Protection and Information Commissioner](#).

Legal basis for processing

Under local privacy laws, there are various grounds which we need to rely on when processing your personal information. The legal basis will depend on the information concerned and the specific context and collection purposes.

For individuals in the EEA and UK or another jurisdiction which prescribes similar legal basis requirements, our legal basis for collecting and using the personal information, including sensitive personal information, is described in the following tables.

Purposes of processing personal information and legal bases

Legal Basis	How it works
Consent	We will ask for your consent to the extent that it is required by EU, UK or applicable local law. In certain cases, such as background checks, you will be asked to advise the third-party service provider of your consent or withdrawal.
Contract and contractual necessity- processing needed to enter a contract with you or perform the obligations	Processing information to the extent that we need to perform a contract with you, or to take steps at your request prior to entering a contract with you.
Legal Obligation	Processing information to the extent that applicable local law, courts or regulators requires us to process, including under regulatory guidance on how we handle recruitment and customer data.
Legitimate Interests	We rely on this legal basis to the extent that we need to process your personal information for a legitimate reason and none of the grounds above applies. Legitimate interests can include: • Workday's recruitment, employment and corporate legitimate interests. • Workday's and its service providers'

	interests to administer an efficient recruitment process now and in the future. • Improving Workday's cloud services and technology. • Promoting and protecting Workday's values and reputation. We will not rely on this basis where an individual's interests and rights should override. The interests of Workday and third parties are considered alongside individual privacy rights, benefits and potential impacts.
--	---

Table 4: The processing grounds we rely upon to process your sensitive personal information:

Purposes of processing sensitive personal information and legal bases

Sensitive Personal Information Ground	How it Works
Employment law rights and obligations.	We process sensitive personal information only to the extent necessary to comply with local recruitment, employment or social security law(s) (as applicable), or similar legal requirements.
Legal Claims	We process sensitive information only to the extent necessary to comply with and process your sensitive personal information to exercise, establish or defend any legal claims or pursuant to the order of a local EU, UK or other applicable court.
Explicit Consent	We process your information only after we have received your specific and clear consent to do so.

Transferring personal information internationally

We process personal information in the U.S. and other countries outside your job application location. Local importer privacy laws can be different to your home location.

When we transfer personal information across international borders, we take measures to protect it. We consider your fundamental rights and freedoms under applicable local laws. We use industry approved standards to assess and put in place appropriate and equivalent data protection levels, e.g.:

- **Countries and Recipients with Adequacy Findings:** The recipient may be in a country that has been found to provide adequate data protection levels based on the adequacy decisions of competent authorities. For personal information transfers within the Workday group to the U.S., Workday, Inc. is certified to import personal information under the DPF.
- **Using Model Clauses.** We also enter "standard contractual clauses" ("SCCs") with data importers. SCCs are terms approved by competent authorities in the EEA, UK, Switzerland and many other global locations, as industry approved safeguards for cross border processing. You may have a right to request a copy of the SCCs. You can use the details in the "[Want to Contact Us?](#)" section.

Vietnam

If you're located in Vietnam, please note the following additional disclosures:

Your consents

We will obtain your consent for our processing of your personal information, if required by Vietnam law, e.g.:

- when changes to this Statement require your consent under local law
- in circumstances where Vietnamese law mandates consent, regardless of any other provisions in this Statement.

Methods of processing personal information

Our processing includes various automated and manual methods, such as collection, recording, analysis, storage, access, retrieval, copying, sharing, transmission, provision, transfer, deletion, and other methods permitted by Vietnamese law.

Additional rights and obligations

In addition to the rights set out in "What are your privacy rights?" section, data subjects have the following rights and obligations, unless otherwise provided by Vietnamese law:

Rights:

- Be informed of the processing of your personal information
- Consent to the processing of your personal information
- Make denunciations, initiate lawsuits, and request compensation for damages in accordance with the applicable law.

Obligations:

- Protect your own personal information; request relevant organizations and individuals to protect your personal information
- Respect and protect others' personal information
- Participate in dissemination of personal information protection skills
- Comply with regulations on personal information protection and prevent violations of personal information protection regulations.

Retention of personal information

Your personal information will be processed from the moment we collect it. It will be processed for the durations described in "How long does Workday retain your personal information?".

Potential consequences and damages of data processing

We take the security of your personal information seriously and apply robust measures to protect it. However, no security system is completely immune to breaches. Despite our efforts, there is a residual risk of unauthorized access, disclosure, or accidental loss, which could lead to data leakage, financial loss, or other adverse impacts. We encourage you to remain vigilant and take appropriate precautions when sharing personal information.