



Patterson Candidate and Employee Privacy Notice

Does this Notice Apply to You?

This Privacy Notice ("Notice") describes how Patterson Companies, Inc. and its subsidiaries (collectively, "we", "us", "our" or "Company") collect and use your personal information. This Notice applies in the following circumstances:

- (1) You apply for an employment position with us;
- (2) You are employed by one of our partners, but are assigned to or supporting the Company;
- (3) We source your information from an unaffiliated third-party company, for example, if we find you on a professional social media site; or,
- (4) You have accepted an offer of employment with us.

Purpose of this Notice

Our workforce is one of our largest investments and ensuring we maintain your trust and our reputation as an employer-of-choice is through responsible data practices. This Notice provides you an overview of how we use and collect your personal information from the time you submit an application, one of our talent sources identifies you as a great fit for an open role, or you find us at a job event. We provide you this Notice to meet legal requirements and because the privacy of your personal information is important to us.

This Notice explains (1) what personal information we collect about you, (2) how we use this information, (3) how we protect and manage this information, and (4) your rights to this information.

Information We Collect About You

We collect, use, and maintain (collectively "process") different types of personal information about you in the regular course of business operations.

If you are a prospective employee, job candidate or applicant, we process your personal information to determine your qualifications and fit for employment with the Company. This may include interview assessments, background screenings, and other screening methods.

As an employee, we process your personal information, including your dependents, beneficiaries and other individuals associated with your employment, to manage our employment relationship with you and your workplace facilities/information systems interactions. For example, to manage or maintain your benefits, we may need to collect personal information about your spouse, domestic partner, or children to extend those benefits to them.



If you are employed by one of our partners, we process your personal information to maintain your engagement and access to our facilities and information systems.

The categories of personal information we process can include the following:

Name and contact information. Your first and last name, employee identification number, email address, mailing address, personal phone number, photo, beneficiary and emergency contact details, and other contact data.

National identifiers. Your national ID/passport, citizenship status, residency and work permit status, social security number, or other taxpayer/government identification number.

Employment details. Your job title/position, office location, offer letter, hire date, termination date, salary or hourly rate of pay, performance history and disciplinary records, leave of absence, sick time, and vacation/holiday records.

Spouse/partner and dependents' information. Your spouse and dependents' first and last names, dates of birth, and contact details. This information is usually always collected and processed for benefits administration.

Reference information. Name, title, contact information for those you may use as references for your employment with us.

Background information. Academic and professional qualifications, education, CV/Resume, and where permissible under applicable laws, criminal records data.

Learning and Development. We collect information related to your learning and development through our various tools, such as late completion of mandatory trainings.

Health Information. Height, weight, health status, or treatment information provided directly by you such as through a pre-employment physical, or through a qualified health program (i.e., medical leave, drug screening, Company sponsored wellness program, etc.).

Video, voice, and image. We may collect and use video, voice and image data about you, subject to the requirements of local law, and any consultation requirements with worker representatives.

Financial information. Bank account details, tax information, salary, retirement account information, company allowances and other information necessary to administer payroll, taxes, and benefits, including expense reimbursement.

Information collected from your use of Company Assets. Emails sent and received, building and information system access, system and application usage when accessing and using our buildings and assets.



Precise Location and Telematics. Depending on your role and responsibilities, if you have access to a Company vehicle, we may collect information such as precise geolocation, driving behavior data, and other vehicle diagnostics such as mileage and service indicator (collectively, “telematics”). We collect telematics data to better manage our vehicle fleet and budget resources. Telematics data is shared with certain third parties as requirements of certain discounts and incentives. If you are impacted by this program, you will receive a separate notice providing more information.

Demographic information. This includes your date of birth and gender identity as well as more sensitive personal information (also known as special category data) including information relating to racial and ethnic origin, religious, political or philosophical beliefs, trade union membership or information about your health, parental status, disabilities, sexual orientation, gender identity, and military status.

We may process this information for a variety of reasons including:

1. Where it is necessary to comply with local requirements and applicable law. For example, we may use this information to comply with anti-discrimination laws and government reporting obligations;
2. To monitor and ensure we maintain accountable for an inclusive work environment through diversity and equality of treatment and opportunity; and,
3. To provide work-related accommodations or adjustments, to provide health and insurance benefits to you and to your dependents.

Where the processing of this information is not required by law, you may choose not to provide that information to us. We will provide a notice at the time the information is collected, and where required, ask for your consent to process your information.

We may also collect personal information about you from **third parties or public sources** as needed to support the employment relationship or to engage with you concerning job opportunities with us. For example, before and during the course of your employment or assignment with us, we may collect information from public social media sources, such as your LinkedIn profile, for recruitment purposes. Also, we may engage with a search firm to fill a role and receive your resume and other personal information through our engagement with that company.

We may conduct background screenings, to the extent permitted by law, through a third-party vendor for information about your past education, employment, credit and/or criminal history. Additionally, if there is an investigation of an employee matter, we may obtain information relevant to the incident from external sources including private parties, law enforcement or public sources like news sources and public social media posts.

How We Use Your Personal Information

We collect your personal information for the purposes listed in this section. In some cases, collection of this information may be optional and you can choose not to provide it; however, in other cases, failure to provide necessary personal information may prevent us from being able to carry out these tasks and/or comply with our legal obligations.



1. To administer your employment, offer letter, or other commitments we've made to you

We process your personal information primarily for the purpose of managing our employment or working relationship with you, to fulfill our contractual or legal obligations, or applicable internal policies, including payroll, benefits administration, pension and retirement administration, and tax reporting. For example, we will need to process your personal information in order to manage our employment relationship with you and pay you.

We may also use information collected from third parties to perform these duties. For example, if you were assigned to us through an assignment at your employer, we may use information provided to us by your current employer to evaluate your fit for a particular role.

We do not use your learning and development information to profile you or create insights related to your fit for a future role, current role, or to evaluate your performance (except as it relates to satisfactory completion of required or mandatory training requirements).

2. Other legitimate business purposes

We also may collect and use your personal information when it is necessary for other legitimate purposes, such as general personnel administration, our workforce directories, to send you gifts, notices or other items, general business management and operations, disclosures for auditing and reporting purposes, internal investigations, management of network and information systems security and business operations, provision and improvement of employee services, physical security and to protect the safety and well-being of employees and others.

Legally required purposes: We may use your personal information when we consider it necessary for complying with laws and regulations, including collecting and disclosing personal data as required by law (e.g., for minimum wage, working time, tax, health and safety, anti-discrimination laws, global migration), under judicial authorization, or to exercise or defend the Company's legal rights.

We use applications and systems that record employee performance metrics, such as sales related or code databases for a variety of purposes, including: business operations; reviewing, rewarding and coaching employees on their performance; administration and assessment of trainings; and, management of Company assets such as vehicles and computers.

When necessary, we process your personal data to investigate potential violations of law or breaches of our internal policies. Every Patterson employee is expected to adhere to our Code of Conduct and an authentic allegation of noncompliance will include an investigation into past activities, communications and -in some cases- travel. Depending on the findings of the investigation, this information may be turned over to law enforcement as evidence. You may not receive advanced notice and you may not object to such sharing.

3. Other uses of your information

Where it is legal to do so, we also may collect your internal usage of our products, services and internal applications and tools including business data created by employees and other staff, to measure and



improve these products; use of your data for product improvement may include human and machine review of the information to train models and improve machine learning for our products and services. Where required by law, we will seek your consent to such uses; and where your consent is sought, we will ensure your consent is knowing, truly voluntary, and that you suffer no adverse consequence from any decision to withhold or revoke your consent.

We commit to only using your personal information for the purposes for which it was collected, unless we reasonably consider that we need it for another purpose that is compatible with the original purpose and there is legal basis for the further processing. For example, you may provide personal information to us while researching job openings, but once you apply for a specific role, we may need to process your personal information based on other legal basis for processing.

Sharing of Your Personal Information

Your personal information may be shared with other third parties, including service providers, for legitimate purposes as follows:

1. In order to carry out the uses of personal information described above (See: [Why We Process Personal Data](#));
2. To enable third parties to provide services to us. Categories of recipients of personal information would include: financial investment service providers; applicant tracking services; insurance providers, pension administrators and other benefits providers; payroll support services; relocation, tax and travel management services; vehicle manufacturers; and, health, quality and safety experts;
3. To comply with our legal obligations, regulations or contracts, or to respond to a court order, administrative or judicial process, such as a subpoena, government audit or search warrant. Categories of recipients would include parties to contracts, judicial and governmental bodies;
4. In response to lawful requests by public authorities (such as national security or law enforcement);
5. To seek legal advice from external lawyers and advice from other professional advisers such as accountants, management consultants, etc.;
6. As necessary to establish, exercise or defend against potential, threatened or actual litigation (such as adverse parties in litigation);
7. Where necessary to protect the Company, your vital interests, such as safety and security, or those of another person;
8. In connection with the sale, assignment or other transfer of all or part of our business (such as a potential purchaser and its legal/professional advisers); or,
9. Otherwise at your direction.

We may share aggregated or de-identified personal information for additional purposes, but those purposes will never identify you or another individual. For example, we may share aggregate data about employee health status with a third party to ensure our employee health program supports everyone's mental and physical well-being.

Workforce Systems Security and Monitoring



We monitor our information technology and communications systems through automated tools such as network authentication and wireless connectivity hardware and software, anti-malware software, website filtering and spam filtering software, security software for cloud-based applications, and mobile device management solutions. The primary purpose of this monitoring is to protect the Company, our employees, customers and business partners, for example, proof of business transactions and recordkeeping; protection of confidential information and company assets; and, investigating allegations of violations of Company policy or laws.

We also monitor our offices, and other work locations and facilities, through video monitoring like closed-circuit television ("CCTV") and badge scans for security purposes.

You should be aware that any message, files, data, document, facsimile, audio/video, social media post or instant message communications, or any other types of information transmitted to, through or from, received or printed from, or created, stored or recorded on our communications systems and assets (included via the use of personal devices accessing corporate IT systems) are presumed to be business-related and may be monitored or accessed by us in accordance with applicable law and workplace agreements (such as works council agreements), and subject to our internal policies concerning access to and uses of such information.

Data Storage and Transfers

Patterson operates physical offices in three countries: United States, Canada, and United Kingdom and as a result, your personal information may need to be transferred to countries outside of where it was originally collected or your country of residence. For example, because we are headquartered in the United States, information collected in other countries is routinely transferred to the United States for benefits enrollment, workforce management, finance and payroll, and several other business related purposes. Generally, we use Model Clauses as our compliance mechanism to transfer personal information subject to UK General Data Protection Regulation to the United States and adequacy for data transfers to Canada.

We retain personal information collected subject to this Notice for as long as necessary fulfill the purposes for which the information was collected and to comply with applicable laws or regulatory requirements. At a minimum, we retain your personal data for as long as you have an active candidate or employment engagement with us.

Data Protection Officer

Patterson Companies has appointed our Chief Compliance and Regulatory Officer as Privacy and Data Protection Officer (DPO). Our DPO is responsible for the strategic vision and direction of our global privacy program and oversees all regulatory engagement related to Patterson's data practices. As of the last revised data, the DPO contact information is:

Name	Shivani Kaul
Title	Chief Compliance & Regulatory Officer
Contact Information	privacy@pattersoncompanies.com



In addition to the information shared above, individuals have certain rights under applicable data protection laws such as the EU General Data Protection Regulation, CPRA, and other localized laws. We refer to these as Data Subject Rights.

State Privacy Rights (California)

If you are a California resident, the California Consumer Privacy Act, as amended by the California Privacy Rights Act (collectively, the "CCPA"), gives you certain additional rights with respect to the personal information we collect about you as a candidate, employee, or individual assigned to or supporting the Company. This section describes those rights and generally describes our practices currently and during the preceding 12 months.

Right to Know. You have the right to request that we disclose the following information covering the 12 months before your request:

1. The categories of personal information we have collected about you;
- 1 The categories of sources from which that personal information was collected;
- 2 The business or commercial purpose for collecting, selling, or sharing personal information;
- 3 The categories of third parties to whom we disclose personal information;
- 4 The categories of personal information, if any, that we sold or shared for cross-context behavioral advertising purposes, and the categories of third parties to whom each was sold or shared; and
- 5 The categories of personal information we disclosed for a business purpose, and the categories of service providers or contractors to whom each was disclosed.

Right to Access. You have the right to request a copy of the specific pieces of personal information we have collected about you.

Right to Delete. You have the right to request that we delete personal information we have collected from you, subject to certain exceptions permitted by the CCPA (for example, where retention is necessary to complete a transaction, comply with a legal obligation, or exercise free speech).

Right to Correct. You have the right to request that we correct inaccurate personal information that we maintain about you.

Right to Opt-Out of Sale or Sharing. California residents have the right to opt out of the "sale" or "sharing" (including for cross-context behavioral advertising) of their personal information, as those terms are defined under the CCPA. We do not sell or share personal information of candidates, employees, or workers assigned to the Company, and have not done so in the preceding 12 months.



Right to Limit Use of Sensitive Personal Information. Where applicable, you have the right to limit our use and disclosure of your sensitive personal information to those purposes permitted under the CCPA.

Right to Non-Discrimination. You have the right to exercise your CCPA rights without discrimination or retaliation, as prohibited by the CCPA.

How to Exercise Your California Rights. You may submit a request to exercise any of the rights above to privacy@pattersoncompanies.com or by phone at 1-800-328-5536. We cannot process your request if you do not provide us with sufficient detail to allow us to understand and respond to it, and we may need to verify your identity (and, where applicable, your California residency) before responding.

Your authorized agent may submit a request on your behalf if you provide the agent with written permission to do so, or a valid power of attorney under California Probate Code Sections 4000-4465, and if the agent can verify its own identity with us. We may still require you to verify your own identity directly with us and to directly confirm that you provided the authorized agent permission to submit the request.

Region Supplemental Notices

The following provisions provide additional details of our privacy program required by certain laws; however, unless otherwise noted, Patterson extends these rights to our global workforce.

United Kingdom – Controller identity and legal bases

Where this Notice applies to individuals in the United Kingdom, National Veterinary Services Ltd. is the controller (as defined in the UK GDPR) for the processing of your personal data described in this Notice.

For each purpose for which we use your personal data, the UK GDPR requires us to have a “legal basis.” Most commonly, we rely on one of the following: (1) where processing is necessary to perform our contract with you (“Contractual Necessity”), for example to administer your employment or offer of employment; (2) where processing is necessary to comply with a legal or regulatory obligation (“Compliance with Law”); (3) where processing is necessary for our legitimate interests, and your interests and fundamental rights do not override those interests (“Legitimate Interests”), such as managing and improving our business, our systems, and our workforce; or (4) where processing is necessary to protect your vital interests or those of another person (“Vital Interest”).

Where we process special category data about you (such as health, trade union membership, or racial or ethnic origin data), we also rely on a condition permitted under Article 9 of the UK GDPR, which, depending on the circumstances, may include: processing necessary to carry out our obligations or exercise our rights in connection with employment (e.g., to assess your working capacity or administer sick pay); processing necessary for reasons of substantial public interest (e.g., equal opportunities monitoring); or processing necessary for the establishment, exercise, or defense of legal claims.



Where necessary, we will collect explicit consent for processing that is not aligned with a legitimate interest. Due to the nature of an employment relationship, some rights are impossible to honor without first terminating the employment relationship. In those instances, you will be informed in writing of the reason for a denial of rights.

Those rights include the right to:

2. Request access to and obtain a copy of your personal information;
3. Request correction of personal information you have provided;
4. Request erasure (or deletion) of personal information that is no longer necessary to fulfill the purposes for which it was collected, or does not need to be retained for other legitimate purposes;
5. Restrict or object to the processing of your personal data; and
6. If applicable, request your personal data be ported (transferred) to another company.

To make a request to exercise one of the above rights, please contact us using one of the methods provided below. We will consider and honor any requests in accordance with applicable data protection laws. To protect your information, we may request specific information from you to enable us to confirm your identity and right to access, as well as to search for and provide you with the personal information that we hold about you. If we charge a fee for this, we will advise you in advance.

We try to respond to all legitimate requests within one month. Occasionally it may take us longer than a month if your request is particularly complex or you have made a number of requests, in which case we will notify you and keep you updated.

Automated decision-making. We do not envisage that you will be subject to decisions that have a significant impact on you based solely on automated decision-making, including profiling.

If we are relying on your consent to process your personal data, you have the right to withdraw your consent at any time. Please note however that this will not affect the lawfulness of the processing before its withdrawal.

You may complain to a data protection authority about our collection and use of your personal information. You may contact your local data protection authority to do so.

If you are in the United Kingdom and feel that your complaint regarding our use of your personal data has not been adequately resolved, you also have the right to make a complaint directly to the UK Information Commissioner's Office (ICO) at <https://ico.org.uk/make-a-complaint/>.

Data security and breach notification. We have put in place security measures designed to prevent your personal data from being accidentally lost, used, or accessed in an unauthorized way, altered, or disclosed, and we have procedures in place to address any actual or suspected personal data breach. Where required by law, we will notify you and an applicable regulator of a breach affecting your personal data.



We are committed to providing transparency to all members of our workforce in our data practices and, certain rights regarding data collected by or otherwise held by us about you. You may also request that we:

- (1) provide you a copy of the personal information we have about you,
- (2) request that we delete the personal information we have about you,
- (3) opt-out of certain processing of sensitive personal information or automatic decision making,
- (4) opt-out of the selling or sharing of personal information, and
- (5) you may elect to appoint an Authorized Agent submit these requests on your behalf.

To do so, you may submit the request by one of the methods listed in the Contact Us section, below. You will be asked to verify your identify before we take action on your request. Additional documentation may be required if you choose to have an Authorized Agent (California residents only) submit this request for you. We will not discriminate against you for exercising your data rights as permitted under applicable law.

Please note that our legal obligations to retain certain data may override your legal rights to delete that information. For example, we may be unable to delete information related to your health benefits because of our compliance obligations under other laws. Similarly, we are unable to honor a delete request during active employment. If we deny your request to exercise your right, we will inform you why the request was denied.

You may view the Right to Know chart which provides more details about the processing of your personal information.

You may submit your requests or questions related to these rights to privacy@pattersoncompanies.com or by phone at 1-800-328-5536.

Contact Us

If you have a privacy concern or question related to this Notice, you may contact privacy@patterson.com or write to us at:

Patterson Companies
Attn: Privacy Officer
1031 Mendota Heights Road
Saint Paul, MN 55120
Telephone: (+1) 800.328.5536

Patterson will never discriminate against you for exercising your data rights. This includes restricting or limiting otherwise permissible access to our Products or Services.

Updates to this Notice



From time to time, it may be necessary for us to update this Notice with more relevant information or to otherwise comply with legal obligations. When we make updates, we will notify you in advance of material changes and maintain previous versions in compliance with our retention schedules.

Last Updated:

October 2026

Previous:

October 2024

December 2022.