Darden Privacy Notice for Team Members and Applicants

Effective Date: January 1, 2023
Updated: May 24th, 2023

Darden and its family of restaurants (**"Company," "we,"** or **"us"**) value your trust and are committed to the responsible collection, management, use, and protection of personal information. We refer to such information as "**Personal Information.**"

This Darden Privacy Notice For Team Members and Applicants (the "**Notice**") provides you with information about how Darden and its family of restaurants ('the Company") collect, use, process, and disclose Personal Information in association with your relationship with the Company as our former, current, and potential employees, contractors, temporary workers, interns, and their family members and dependents (collectively, "**Personnel**"). This Notice describes the Personal Information, the ways in which we may share such information, and the Personnel's rights regarding processing Personal Information.

Click on one of the links below to jump to the listed section:

What Types of Information Do We Collect?

In the course of your employment with or application for employment with us, or contractor-related activities, we may need to collect personal information about you and may collect information about your spouse, domestic/civil partner, or dependents ("**Dependents**"), to establish, manage, terminate, or otherwise administer the relationship. Your personal information may also be used for internal administration and compliance with legal and regulatory obligations.

The Personal Information we collect may include the following, but are not limited to:

- **Identifiers:** Name, employee identification number, work, and home contact details (email, phone numbers (including mobile), fax numbers, physical address), language(s) spoken, national identification number, social security number, dependents, emergency contact information, nationality, images or photographs, and information that may relate to other protected characteristics.
- **Demographics Information:** Gender, age, date of birth, race, color, sexual orientation, religion, national origin, genetic, marital/civil partnership status, spouse or domestic partners, military service, disability status, and biometric information (e.g., face geometry, fingerprint, voice recording).

- **Financial Information:** Base salary, bonus, employee benefits and allowances, long-term compensation awards, total compensation, pay period, compensation rate, benefit plan enrollments and entitlements, benefit election statements, compensation type, stock option awards and grants, details of any shares of common stock or directorships, restricted stock share awards and grants, performance unit awards and grants, shares purchased in the employee stock purchase plan, other company equity grants, currency, pay frequency, compensation history, effective date of current compensation, salary reviews, banking details, bank account number, tax identification number, and related information, tax location code, working time records (including vacation and other absence records, leave status, hours worked and standard department hours), payroll identification number and payroll, and overtime eligibility and overtime pay.
- **Geolocation Data**: Precise geographic location information about a particular individual or device (e.g., device location, VPN location).
- **Work Eligibility Information:** Citizenship, immigration status, passport or visa data, details of residency or work permit, and Employment Eligibility Verification.
- **Information Relevant to Matters of Public Health:** Health information, symptoms, vaccination status, test results, close contact, and exposure information, as is relevant to monitor and respond to requests or report on matters deemed relevant to public health.
- **Internet or Other Electronic Network Activity Information:** Information required to access the Company systems, network, resources, and applications such as IP addresses, log files, electronic communications and files, network connections, login credentials, email account (team member incoming and outgoing emails (business and personal)), incoming and outgoing text messages, browsing history, search history, and information regarding a team members interaction with an internet website, social media postings, application, or advertisement, instant messaging account, mainframe ID, previous employee ID, previous manager-employee ID, system passwords, and electronic information produced by you using Company systems.
- **Professional or Employment Related Information:** Description of current position, title, status, management category, business unit, job code, salary plan, pay grade or level, job function(s) and subfunction(s), company name and code, legal employer entity, branch/unit/department name and code, location, employment status and type, full-time/part-time, terms of employment, employment contract, severance plan and eligibility data, internal and external job and work history, job responsibilities, hire/rehire and termination date(s) and reason, promotion dates, employee class length of service, retirement eligibility, disciplinary records, date of transfers, reporting manager(s) information, subordinate employee information, details contained in letters of application, resumes, and CVs (information necessary to complete a background check), detailed performance and development reviews, ratings and comments, opinions expressed about you, and information used to populate employee biographies, including likes, dislikes and interests. Travel and transaction details for business-related travel and expenses, including travel reservation numbers if issued, expense reimbursement information, credit card numbers, and transactions; travel information (airline, flight number, hotel name, dates of travel). Name, position, and contact information of the team member making a complaint, the individuals who are the subject of the complaint or an investigation, the persons investigating the complaint, the facts collected, and the investigation results.
- **Education Information:** Education history, professional qualifications, language, and other relevant skills, certifications, certification expiration dates), assessments, assessment results, training and development programs planned, attended, and completed, and web-based training programs.
- **Audio/Visual Data:** Audio, electronic, visual, thermal, olfactory, or similar information such as CCTV images and photographs, video recordings in certain work areas and photographs for identification purposes, and audio recordings (e.g., recorded meetings and webinars, recordings of communications for quality control, record-keeping, and training purposes).
- **Inferences drawn from the information above:** Preferences or characteristics related to a position at Darden.

Some of the information we collect may be deemed sensitive information (e.g., government identifiers, login credentials, precise geolocation, race or ethnic origin, sexual orientation, union membership, religious or philosophical beliefs, contents of communications sent or received via our IT systems, biometrics, and information regarding health). Darden does not process such personal information to infer characteristics about You.

Why Do We Collect Personal Information?

We collect, use, transfer, and disclose Personal Information for one or more of the following purposes:

Recruitment

If you apply for or are recommended for a role at the Company, we collect, use, and share personal information for recruitment purposes:

- To evaluate your qualifications for employment and to reach a hiring decision. This includes assessing your skills, qualifications, and background for a particular role, verifying your information, carrying out reference or background checks, checking visa status and/or eligibility to work (where applicable), and generally managing the hiring process and communicating with you about it.

- If you are accepted for a role at the Company, the information collected during recruitment will form part of your ongoing record.

- If you are not offered a position, we may retain your Personal Information to allow us to consider you for other suitable openings within the Company in the future.

Employment or Work-Related Purposes

If Company employs you, we collect, use, and share Personal Information for the following purposes:

- **Workforce Management:** Includes managing work activities and personnel, including recruitment, appraisals, performance management, promotions and succession planning, rehiring, administering salary and compensation administration and reviews, wages, bonuses, and other awards, equity plan (such as stock options, stock grants, and employee stock purchase plan) participation and administration, processing accounts payable and receivable for employees healthcare benefits, pensions, and savings plans, training, leave, managing disability and sickness leave, promotions, transfers, secondments, honoring other contractual benefits, providing employment references, loans, performing workforce analysis and planning, performing employee surveys, performing background checks, managing disciplinary matters, grievances, and terminations, reviewing employment decisions, making business travel arrangements, managing business expenses and reimbursements, planning, and monitoring training requirements and career development activities and skills, and creating and maintaining one or more internal employee directories.
- **Workforce Analytics**: For succession planning, workforce management, and data security. For Instance, we use workforce analytics to assist in planning succession and to ensure business continuity, to design team member retention programs and diversity initiatives, to offer training opportunities, and to identify patterns in the use of technology; systems to information entrusted to us as well as to protect our associates and property.
- **Communications and Emergencies:** Including facilitating communication with you, ensuring business continuity, property management (e.g., laptops and mobile phones), providing references, protecting the health and safety of associates and others, safeguarding IT infrastructure, office equipment, and other property, facilitating communication with you, your nominated contacts in an emergency.
- **Business Operations:** For operating and managing the IT and communications systems (including email collection, storage, and review), managing product and service development, improving products and services, managing company assets, allocating company assets and human resources, strategic planning, project management, business continuity, a compilation of audit trails and other reporting tools, maintaining records relating to business activities, budgeting, financial management and reporting, communications, managing mergers, acquisitions, sales, reorganizations or disposals and integration with the purchaser.
- **Complying with legal and other requirements:** Such as income tax deductions, record-keeping, reporting obligations, conducting audits, compliance with government inspections and other requests from government or other public authorities, responding to legal processes such as subpoenas, pursuing legal rights and remedies, defending litigation and managing any internal complaints or claims, conducting investigations, including team member reporting of allegations of wrongdoing, policy violations, fraud, or financial reporting concerns, and complying with internal policies and procedures.
- **Monitoring Use of Technology:** We collect information about the use of Company information, assets, and resources, including internet access, electronic communications, and application usage. We collect this information to assess compliance with applicable laws and policies, to protect Company resources against unauthorized access, and to prevent crime and fraud.

We neither share for targeted advertising nor sell the personal information we collect regarding Personnel, including sensitive personal information and information associated with Personnel under 16 years of age.

Retention of Personal Information

We will retain your Personal Information for the time period required or permitted by law, or for the time reasonably necessary to achieve the purposes described in this Privacy Notice or any other notice provided at the time of collection. Retention is based on several factors, including:

- The business purposes for which the information is used, and the length of time for which the information is required to achieve those purposes;
- The existence of an ongoing relationship between you and us;
- Record keeping, the statute of limitations, or legal compliance requirements;
- The need to resolve inquiries or complaints; and
- Protecting the rights or safety of you, us, or others.

How We Collect Personal Information

We may obtain personal information about You from the following categories of sources:

- Directly from you, during recruitment and hiring (e.g., the application form that you complete during the recruitment process, in interviews, or through the completion of any tests or surveys);
- Other individuals, for example, in connection with hiring referrals, references, provision of benefits, feedback from guests or business partners;
- Our affiliates and subsidiaries;
- Service providers, contractors, and other vendors who provide services on our behalf;
- Internet service providers;
- Operating systems and platforms;
- Government entities;
- Social networks (e.g., LinkedIn, Indeed); and
- Data brokers (e.g., background check services)

To the extent we process de-identified information, we will maintain and use the information in de-identified form and will not attempt to re-identify the information unless permitted by applicable law.

How Do We Share Personal Information?

We may disclose all of the categories of Personal Information listed above for our business purposes. The categories of recipients include:

- **Service Providers**: Companies that provide products and services to the Company and our team members, such as payroll; human resources services, performance management, training, expense management, IT systems suppliers and support; third parties assisting with equity compensation programs, credit card companies, medical or health practitioners, trade bodies and associations, travel agents and other service providers**.**

- **Benefit providers**: We will arrange for you to receive certain benefits from third parties, such as insurance or financial benefits companies. The Company may share information with those parties to facilitate the provision of those services.

- **Consultants**: We may provide Personal Information to consultants and advisors that help us operate and improve our business.

- **Group companies**: We have affiliates around the world. We may disclose your personal information to affiliates for employment, recruiting, security, and internal reporting purposes. Unless otherwise specified, Company affiliates will only use your information in the ways described in this Notice.

- **Recipients of legal disclosures**: We may disclose your Personal Information to law enforcement agencies, courts, other government authorities, or other third parties where we believe necessary to comply with a legal or regulatory obligation. Company may disclose Personal Information as we deem reasonably necessary to support lawful investigations or requests, or as reasonably necessary to protect our rights or the rights of you or any other party.

- **Professional Advisors**: Accountants, auditors, lawyers, insurers, bankers, and other outside professional advisors who help support Company operations.

- **Public and Governmental Authorities**: Entities that regulate or have jurisdiction over the Company, such as regulatory authorities, law enforcement, public bodies, and judicial bodies.

- **In the context of a transaction**: We may also share Personal Information in connection with any proposed or actual reorganization, merger, sale, joint venture, assignment, transfer, or other disposition of all or any portion of the Company business, assets, or stock (including in connection with any bankruptcy or similar proceedings).

Your California Privacy Rights

This section pertains to employees or candidates that reside in California and supplements information regarding the collection, use, and disclosure in this Privacy Notice.

California residents have specific rights regarding their Personal Information under the California Privacy Rights Act ("CPRA") as described below and subject to certain exceptions.

To process your rights, we will ask for your full name, email address, date of birth, and employee ID number (if available). Please note that we may require additional information from you in order to honor your request, and we may decline your request as permitted under applicable law.

Right to Know

You have the right to request access to Personal Information collected about you and information regarding the source of that Personal Information, the purposes for which we collect it, and the third parties and service providers with whom we disclose it.

You or your authorized agent may exercise this right by submitting a verifiable employee request to us by either:

- Submitting your request here
- Calling 1-888-467-4123

Right to Delete

You also have a right to request that we delete your Personal Information.

You or your authorized agent may exercise this right by submitting a verifiable employee request to us by either:

- Submitting your request here
- Calling 1-888-467-4123

Right To Correct
You have the right to request that any inaccurate or incomplete Personal Information held by us or on our behalf is corrected by contacting us. We will take reasonable steps to ensure the accuracy of the Personal Information we retain about you. It is your responsibility to ensure you submit true, accurate, and complete information to us and timely update us in the event this information changes.

You or your authorized agent may exercise this right by:

- Submitting your request here
- Calling 1-888-467-4123

Right to Non-Discrimination
You have the right not to receive discriminatory treatment for exercising any of your CCPA rights. Unless permitted by the CCPA, we will not:

- Deny you services.
- Charge you different prices or rates for services, including through granting discounts or other benefits or imposing penalties.
- Provide you with a different level or quality of services.
- Suggest that you may receive a different price or rate for services or a different level or quality of services.

How to Contact Us

If you have questions about this privacy notice or our privacy practices, please send an email to our Privacy Team at Privacy2@darden.com or send a letter to:

Darden Restaurants
Attn: Ethics & Compliance-Privacy
1000 Darden Center Drive
Orlando, FL 32837

Team Member's Obligations

Please keep your Personal Information up to date and inform us of any significant changes to your Personal Information. You agree to inform your Dependents whose Personal Information you provide to the Company about the content of this Notice.