

Dine Brands Global, Inc. Applicant and Employee Privacy Notice

Last Updated/Effective Date: April 1, 2023

1.0 Introduction

In this Applicant and Employee Privacy Notice ("**Notice**"), Dine Brands Global, Inc. and its subsidiaries and affiliates ("**Dine Brands**", "**we**", or "**us**") describe the types of information that we collect from job applicants and current and former employees, how we use that information, and how we may share that information.

This Notice applies to current and former Dine Brands employees as well as applicants to open positions at Dine Brands. This Notice does not form a part of any contract of employment offered to job applicants hired by Dine Brands. Provisions of this Notice dealing with individuals employed with Dine Brands are not applicable until they begin working for us.

We may change this Notice from time to time, and we will post changes in an area of our website that is accessible to current and former Dine Brands employees.

When you apply to work for Dine Brands via one of our websites ("**Sites**"), you will be re-directed to our third-party service provider (e.g., Workday). Our third-party service provider will provide us with the information necessary for us to consider your application. Any information that you provide directly to our third-party service provider is governed by its privacy policy.

2.0 Categories of Personal Information We Collect

We may collect a range of Personal Information. "Personal Information" means information that uniquely identifies, relates to, describes, or is reasonably capable of being associated with or linked to you. We collect the following types of Personal Information when you apply for a job with Dine Brands or during the course of your employment at Dine Brands:

- Your name, address, email address, telephone number, and other contact information;
- Your resume or CV, cover letter, previous and/or relevant work experience, or other experience, education, transcripts, or other information you provide to us in support of an application and/or the application and recruitment process;
- Information from interviews you may have, if any;
- Details of the type of employment you are looking for, current and/or desired salary, other terms relating to compensation and benefits packages, and job preferences;
- Details of how you heard about the position you are applying for;
- Any sensitive and/or demographic information obtained during the hiring process such as Social Security number, gender, information about your citizenship and/or nationality, medical or health information, and/or your racial or ethnic origin;
- Reference information and/or information received from background checks (as applicable), including information provided by third parties;

- Information relating to any previous applications you may have submitted to Dine Brands and/or any previous employment history with Dine Brands;
- Information about your educational and professional background from publicly available sources that we believe is relevant to your application or a potential future application (e.g., your LinkedIn profile);
- Banking information for direct deposit purposes, income history, income information, benefits information, and information regarding your beneficiaries; and
- Information collected from you automatically when you use our Sites, while using a Dine Brands device, or while connected to Dine Brands' internet through cookies, web beacons, pixel tags, and other online tracking mechanisms.

3.0 Information Collected From Other Sources

We obtain information about individuals from various third-party and public sources, and we may combine that data with Personal Information we have. For example:

- Dine Brands may collect application information from recruiters;
- Dine Brands may collect information regarding your past employment (including performance information) from former employers;
- Dine Brands may collect information regarding your citizenship or eligibility to work in the country where you would be employed from government agencies;
- Dine Brands may collect your credit history and/or criminal record if you consent to a credit check or background check;
- Dine Brands may collect information relating to your qualifications to work with Dine Brands from your references;
- Dine Brands may collect your drug test results from the third-party services provider Dine Brands uses to perform applicant and employee drug tests; and
- Dine Brands will collect tax related information from the Internal Revenue Service.

4.0 Children Under 18

We only employ those who are legally eligible to work at the location of employment, which is typically the age of majority (18 years old). Please do not send us application materials if you are under the legal age eligible for employment.

5.0 Purposes for Which We Collect Personal Information

Dine Brands processes your Personal Information as described in this Notice for the following purposes:

- **To manage the application process.** We use your Personal Information to process your job application, verify the information you have provided in your application, communicate with you regarding your application, answer your questions regarding the application process, and confirm your eligibility for a position. We may also save your information for future job openings within Dine Brands.

- **To manage the hiring process.** We may use your Personal Information in the hiring process to conduct interviews. We may also use your Personal Information to perform background and reference checks—with your consent—if you are offered a position.
- **To communicate with you.** We may use your Personal Information to provide information to you, respond to your questions, notify you of changes to your compensation and benefits program, or notify you of emergencies.
- **To manage the onboarding process.** Upon being hired by Dine Brands, we will collect Personal Information when you complete new hire paperwork to assist us in administering salary and benefits and to assist us with complying with governmental and legal requirements.
- **To administer compensation and benefits programs.** We will use the Personal Information you provide to process payroll, pay taxes, help employees address employment-related tax issues, administer benefits, and handle work-related expense reimbursements. We may also use this Personal Information to manage requests for accommodation requests. We also use this to administer employee claims such as workers' compensation or unemployment benefits.
- **Recruiting.** We may use Personal Information to communicate with you regarding the recruiting process, learn where you heard about Dine Brands, and evaluate and improve our recruiting process.
- **For performance management.** Dine Brands collects Personal Information in order to assess your performance, assist in career development, conduct pay and grading reviews, and handle any employment-related disputes. We may also use Personal Information to respond to violations of company policies and gather information for disciplinary actions. We may monitor any activity you perform online while using a Dine Brands device or while connected to Dine Brands' internet such as monitoring the websites you visit and your activity on those websites. We may also track the emails you send using your Dine Brands-provided email address, the phone calls you make using a Dine Brands-provided device, and the chat messages you are involved in using the Dine Brands-provided instant messaging program.
- **Educational and professional services.** We may use your Personal Information to assist with education, training, and professional development.
- **Law enforcement and courts.** We may disclose your Personal Information in response to a subpoena, a search warrant, or other legally valid process. We may use your Personal Information to cooperate with law enforcement or other government entities if you are suspected of having violated applicable laws.
- **Recordkeeping.** We may use Personal Information to comply with applicable legally required or industry standard business and employment recordkeeping requirements and to respond to governmental requests for information.
- **Health and safety.** We use Personal Information to protect your health and safety or the health and safety of others, including the use of technology to allow contact tracing if you may have been exposed to communicable diseases such as COVID-19. We may also use this information to respond to an employee-related emergency. We also use this Personal Information to protect our facilities and personal property.
- **Protect our legal rights.** We may use your Personal Information to protect our legal rights, defend a claim or lawsuit, and investigate or prevent actual or suspected loss or harm to persons or property. We may use your Personal Information to seek legal,

accounting, or other professional advice. We may use your Personal Information when necessary to identify, contact, or bring a legal action against someone who may cause or be causing harm to, or interfering with the legal rights of, Dine Brands or any other party.

- **Security.** We may use your Personal Information to monitor the use of our information systems and electronic resources, to conduct internal audits or investigations, and for the safety and security of Dine Brands employees, visitors, and facilities. We also may use such information to protect Dine Brands against illegal activity and misconduct such as fraud, deceptive practices, and security investigations. We use this to offer, operate, maintain, deliver, troubleshoot, and update the Sites, programs, network, and systems used by Dine Brands in the course of its business.

6.0 How We Share Your Personal Information

We may share your personal information in the following circumstances:

- **Within Dine Brands.** We may share your personal information internally within Dine Brands and among Dine Brands' affiliates for purposes of recruiting and/or evaluating applicants, resource planning, talent retention, human resources, and business administration functions. All Dine Brands employees who access or process applicant personal information are required to comply with Dine Brands' privacy and security policies.
- **Service providers.** We may share your personal information with third parties that help us provide and administer our talent and recruiting, human resources, and business functions.
- **Legal requirements.** We will cooperate with law enforcement and other governmental agencies. We may disclose Personal Information for the following legal purposes:
 - If we believe in good faith we are legally required to disclose that Personal Information.
 - If we are advised to disclose Personal Information by our legal counsel.
 - When necessary to identify, contact, or bring a legal action against someone who may cause or be causing harm to, or interfering with the legal rights of, Dine Brands or any other party.
 - For tax and payment purpose (e.g., Internal Revenue Service).
 - To protect our rights or property, your health and safety, or the health and safety of others.
 - To detect and investigate fraud or illegal activity or to respond to a government request.
 - To respond to an emergency.
- **Professional advisors.** We may share Personal Information with our professional advisors, such as our attorneys and accountants, in their capacity as advisors, including for advice on potential or actual litigation matters.
- **Change in ownership.** We may use and disclose Personal Information in connection with the evaluation of a change of control of Dine Brands such as in the event of a merger, acquisition, or sale of assets. We may provide Personal Information in

connection with a due diligence process, or it could be transferred as part of the change in control to subsequent owner(s). If we (or our assets) are acquired or if we go out of business, enter bankruptcy, or go through some other change in control or reorganization, Personal Information and other information could be one of the assets transferred to or acquired by a third party or reviewed as part of the due diligence process.

7.0 De-Identified/Aggregate Information

We may collect or create information that is de-identified or aggregate information that does not identify a natural person ("**De-Identified Information**"). Dine Brands is the sole and exclusive owner of De-Identified Information and may use or share such information for any legal business purpose. For example, Dine Brands may create aggregate information about applicants to learn about the success of its recruiting processes.

8.0 Data Security

Dine Brands makes commercially reasonable efforts to protect employees' and applicants' Personal Information. We protect Personal Information using technical and organizational measures designed to reduce the risks of loss, misuse, and unauthorized access, disclosure, alteration, and destruction of Personal Information appropriate to the type of Personal Information processed.

Notwithstanding our security safeguards, it is impossible to guarantee 100% security in all circumstances. Dine Brands employees and applicants are responsible for safeguarding the security of any password, user ID, or other forms of authentication involved in obtaining access to password-protected or secure areas of any Dine Brands-owned or licensed platforms. It is your sole responsibility to use the appropriate level of care whenever communicating with us.

If you have reason to believe that your interaction with us is no longer secure, you must immediately notify us of the problem. If a breach of your Personal Information occurs, we will notify you of the breach if and as required under applicable law. In order to protect you and your Personal Information, Dine Brands may suspend your use of any Dine Brands programs or platforms without notice pending an investigation if any breach of security is suspected.

9.0 Retention of Your Personal Information

Personal Information will be stored in accordance with applicable laws and kept as long as needed to carry out the purposes described in this Notice or as otherwise required by applicable law, taking into consideration any statutorily required minimum periods of time in applicable jurisdictions. Generally, this means your Personal Information will be retained until the end of your employment or work relationship with us plus a reasonable period of time thereafter to respond to employment or work-related inquiries or to deal with any legal matters, document the proper termination of your employment or work relationship, or to provide you with any ongoing benefits.

Personal Information which is no longer to be retained will be securely and effectively destroyed or permanently erased from our systems, and we will also require third parties to destroy or erase such Personal Information where applicable.

10.0 California Privacy Notice

This Section applies to our collection and use of “Personal Information” if you are a resident of California, as required by the California Consumer Privacy Act of 2018 and its implementing regulations (“CCPA”), as amended by the California Privacy Rights Act (the “CPRA”), where “Personal Information” has the definition set forth in the CCPA, as amended by the CPRA. This Section describes (1) the categories of Personal Information collected and disclosed by us, (2) your privacy rights under the CCPA, as amended by the CPRA, and (3) how to exercise your rights.

10.1 Categories of Personal Information

Dine Brands makes the following disclosures regarding Personal Information it has collected within the last 12 months:

<u>Category of Personal Information</u>	<u>Collected</u>	<u>Category of Source from which Personal Information is Collected</u>	<u>Purpose of Collection</u>	<u>Third Parties to whom Personal Information is Disclosed for a Business Purpose</u>	<u>Third Parties to whom Personal Information is Sold or Shared</u>	<u>Retention Period</u>
Identifiers.	Yes.	Directly from employees/applicants.	See Section above titled “Purposes for Which We Collect Personal Information”.	Data storage providers, website or mobile application hosting providers, and e-mail service providers.	We do not sell or share this category of Personal Information.	Applicants: 3 years. Employees: Length of your employment plus 8 years.

Personal information categories listed in the California Customer Records statute (Cal. Civ. Code § 1798.80(e)).	Yes.	Directly from employees/applicants.	See Section above titled "Purposes for Which We Collect Personal Information".	Data storage providers, website or mobile application hosting providers, and e-mail service providers.	We do not sell or share this category of Personal Information.	Applicants: 3 years. Employees: Length of your employment plus 8 years.
Protected classification characteristics under California or federal law.	Yes.	Directly from employees/applicants.	See Section above titled "Purposes for Which We Collect Personal Information".	Data storage providers, website or mobile application hosting providers, and e-mail service providers.	We do not sell or share this category of Personal Information.	Applicants: 3 years. Employees: Length of your employment plus 8 years.
Commercial information.	No.	N/A.	N/A.	N/A.	N/A.	N/A.
Biometric information.	No.	N/A.	N/A.	N/A.	N/A.	N/A.
Internet or other similar network activity.	Yes.	Cookies and other tracking technologies.	See Section above titled "Purposes for Which We Collect Personal Information".	Data storage providers, website or mobile application hosting providers, and e-mail service providers.	We do not sell or share this category of Personal Information.	Varies depending on the website and the type of cookie collecting this PI, but generally no more than 2 years. One exception is a cookie associated with the Sitecore Content Management System, used for web analytics to identify repeat

						visits by unique users, that has a lifespan of 10 years.
Geolocation data.	No.	N/A.	N/A.	N/A.	N/A.	N/A.
Sensory data.	No.	N/A.	N/A.	N/A.	N/A.	N/A.
Professional or employment-related information.	Yes.	Directly from employees/applicants; third-party sources (See "Information Collected From Other Sources" section above).	See Section above titled "Purposes for Which We Collect Personal Information".	Data storage providers, website or mobile application hosting providers, and e-mail service providers.	We do not sell or share this category of Personal Information.	Applicants: 3 years. Employees: Length of your employment plus 8 years.
Non-public education information (per the Family Educational Rights and Privacy Act (20 U.S.C. Section 1232g, 34 C.F.R. Part 99)).	No.	N/A.	N/A.	N/A.	N/A.	N/A.
Inferences drawn from other Personal Information.	No.	N/A.	N/A.	N/A.	N/A.	N/A.

Sensitive Personal Information.	Yes.	Directly from employees/applicants.	See Section above titled "Purposes for Which We Collect Personal Information".	Data storage providers, website or mobile application hosting providers, and e-mail service providers. Dine Brands does not use or disclose Sensitive Personal Information other than to facilitate its recruitment and employment operations.	We do not sell or share this category of Personal Information.	Applicants: 3 years. Employees: Length of your employment plus 8 years.
---------------------------------	------	-------------------------------------	--	--	--	--

10.2 CCPA/CPRA Rights

If you are a resident of California, you have the following rights:

Privacy Right	Description
Notice	The right to be notified of what categories of Personal Information will be collected at or before the point of collection and the purposes for which they will be used and shared.
Access	The right to request the categories of Personal Information we have collected about you; the categories of sources from which the Personal Information was collected; the business or commercial purpose for collecting, selling, or sharing Personal Information; the categories of third parties to whom we disclosed Personal Information to; and the specific pieces of Personal Information we have collected about you in the twelve (12) months preceding your request for your Personal Information.
Deletion	The right to have your Personal Information deleted. However, please be aware that we may not fulfill your request for deletion if we (or our service provider(s)) are required or permitted to retain your Personal Information for one or more of the following categories of purposes: (1) to complete a transaction for which the Personal Information was collected, provide a good or service requested by you, or complete a contract between us and you; (2) to ensure our website integrity, security, and functionality; (3) to comply with applicable law or a legal obligation, or exercise rights under the law (including free speech rights); or (4) to otherwise use your Personal Information internally, in a lawful manner that is compatible with the context in which you provided it.

Correction	You have the right to request that we correct any incorrect Personal Information that we collect or retain about you, subject to certain exceptions. Once we receive and confirm your verifiable consumer request (see below), we will correct (and direct any of our service providers that hold your data on our behalf to correct) your Personal Information from our records, unless an exception applies. We may deny your correction request if (a) we believe the Personal Information we maintain about you is accurate; (b) correcting the information would be impossible or involve disproportionate; or (c) if the request conflicts with our legal obligations.
Automated Decision Making	You have the right to request information about the logic involved in automated decision-making and a description of the likely outcome of processes, and the right to opt out. Dine Brands does not currently engage in any automated decision-making practices as it pertains to your employment.
To Opt Out of Sales or Sharing of Personal Information	We do not sell or share your Personal Information as it relates to your employment with Dine Brands. However, if we did, you would have the right to opt out of the sale or sharing of your Personal Information.
Limit Use of Sensitive Personal Information	Dine Brands does not use or disclose Sensitive Personal Information other than to facilitate its recruitment and employment operations. However, if we used or disclosed Sensitive Personal Information for other purposes, you would have the right to opt out.

10.3 CCPA/CPRA Verifiable Consumer Request

To submit a request, please contact us at (866) 926-5019 or complete the privacy web form located [here](#). You may only make a request to exercise your rights on behalf of yourself. You also have a right to submit requests to exercise your rights under the CCPA, as amended by the CPRA through an authorized agent. An authorized agent must be registered with the Secretary of State in California to conduct business in California. If you choose to use an authorized agent, you may be required to: (a) provide signed permission to that authorized agent to submit requests on your behalf, (b) verify your identity directly with Dine Brands, and (c) directly confirm with Dine Brands that you granted permission to the authorized agent to submit the request on your behalf. For clarity, you are required to verify the identity of both yourself and the authorized agent.

If we cannot initially verify your identity, we may request additional information to complete the verification process. We will only use Personal Information provided in a request to verify the requestor's identity. To verify your identity when you or your authorized agent submits a request, we will match the identifying information you provide us to the Personal Information we have about you. Once we receive your request, we will notify you of receipt within 10 days and promptly take steps to respond to your request within 45 days. If we require additional time, we will inform you of the reason and extension period as permitted by the CCPA, as amended by the CPRA. Any disclosures we provide will only cover the 12-month period preceding our receipt of your request.

We cannot respond to your request or provide you with Personal Information if we cannot verify your identity and confirm the Personal Information relates to you. We may deny certain requests, or only fulfill some in part, as permitted or required by law. For example, if you request to delete Personal Information, we may retain Personal Information that we need to retain for legal purposes.

10.4 Non-Discrimination

We will not discriminate against you in the event you exercise any of the aforementioned rights under CCPA, as amended by the CPRA.

10.5 Accessibility

This Notice is available to consumers with disabilities. To access this Notice in an alternative downloadable format, please click [here](#).

11.0 Changes to this Notice

We may change this Notice from time to time, and we will post any changes on this page. Each version of this Notice is identified at the top of the page by its Effective Date.

12.0 Contact Us

For any questions or concerns, please contact us as follows:

Legal Department
privacydesk@dinebrands.com
10 West Walnut Street, 5th Floor
Pasadena, California 91103
(866) 926-5019