GREEN DOT EMPLOYEE CALIFORNIA CONSUMER PRIVACY STATEMENT

Effective and Last Updated: March 2024

Your privacy is important to us. This Green Dot Employee California Consumer Privacy Statement ("**Employee CCPA Privacy Statement**") describes the types of information collected, used, and disclosed by Green Dot Corporation, Green Dot Bank d/b/a GoBank and GO2bank, and their subsidiaries and affiliated companies (collectively, "***Green Dot***," "***we,***" "***us,***" and "***our***") in the context of a person's role as a job applicant, employee, intern, contractor, or other member of Green Dot's workforce ("**Employee Personnel**"). This Employee CCPA Privacy Statement also describes the privacy rights of Employee Personnel that are California residents under the California Consumer Privacy Act of 2018 ("CCPA") and how they can exercise these rights.

This Employee CCPA Privacy Statement applies solely to Employee Personnel that are also California residents and supplements Green Dot's Online Privacy Statement. We may change this Employee CCPA Privacy Statement from time to time. If we do, we will notify you by posting the updated version.

CATEGORIES OF PERSONAL INFORMATION WE COLLECT AND HOW WE MAY DISCLOSE PERSONAL INFORMATION TO THIRD PARTIES

We collect and disclose to third parties the following categories of personal information, as defined in the CCPA, relating to Employee Personnel who are California residents. Note that in addition to the categories of third parties identified in the table, we may disclose your personal information with a potential buyer (and its agents and advisors) in connection with any proposed merger, acquisition, or any form of sale or transfer of some or all of our assets (including in the event of a reorganization, dissolution, or liquidation), in which case, personal information held by us about you will be among the assets transferred to the buyer or acquirer; or we may disclose your personal information to other third parties when we have your consent to do so.

Category of Personal Information	Examples	Categories of 3rd Parties to Whom Personal Information is Disclosed for Business Purposes
Identifiers	Name, email address, postal address, telephone number, social media handles, social security number, driver's license, state identification, passport number, account login credentials, IP address, or other similar identifiers	• Affiliated companies • Government entities and others with whom we share personal information for legal or necessary purposes • Service providers
Contact, health insurance, financial or other personal information	Home address, health or vaccine information, health insurance details, direct deposit or other financial information, and background check information	• Service providers
Protected classifications	Race, age, ethnicity, citizenship, color, marital status, medical condition, sex, gender identity, sexual orientation, and veteran or	• Affiliated companies • Service providers

	military status	
Internet or electronic network activity information	Browsing history, search history, and information regarding an individual's interactions with our website, mobile application, or advertisements, and contents of any mail, email, and text messages sent or received using a corporate device	• Affiliated companies • Service providers
Geolocation data	Device location, including coarse and precise location data	• Service providers
Audio, electronic, visual, similar information	Call and video recordings	• Affiliated companies • Service providers
Inferences drawn about you from other personal information	Certain inferences concerning an individual's preferences, abilities, characteristics and abilities	• Affiliated companies • Service providers
Professional or employment related information	Information such as work history, performance evaluations, payroll and compensation information and survey responses	• Affiliated companies • Government entities and others with whom we share personal information for legal or necessary purposes • Service providers
Education information	Education records and date of graduation	• Affiliated companies • Government entities and others with whom we share personal information for legal or necessary purposes • Service providers

We have not "sold" personal information within the preceding 12 months for monetary value, and we do not "share" (as the term is defined by the CCPA) the personal information of our Employee Personnel.

California Sensitive Information Disclosure. Some of the personal information we collect as described above is considered "sensitive personal information" under California law. We collect the following categories of sensitive personal information (as defined under California law): social security, driver's license, state identification card, or passport number; account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account; precise geolocation; racial or ethnic origin, religious, or philosophical beliefs; contents of mail, email, and text messages sent to business addresses or devices; information concerning health; and information concerning sexual orientation. This information is collected in order to administer your relationship with us, including fulfilling any obligation that we have to provide you with compensation and/or benefits; determine eligibility for employment; conduct background checks (where permitted by applicable law); comply with applicable laws and regulations; create, maintain, and secure online employee accounts; business travel; manage and monitor

employee access to Green Dot facilities, equipment, and systems; investigate and enforce compliance with and potential breaches of the Green Dot's internal policies and procedures; and exercise or defend the legal rights of Green Dot and its employees and affiliates, customers, contractors, and agents.

We collect personal information of Employee Personnel in connection with applications for employment, employment with Green Dot, human resources activities, Green Dot devices, our websites and mobile applications, and Green Dot locations. All personal information and sensitive personal information are used and disclosed by Green Dot for purposes permitted in the CCPA. We do not "sell" or "share" sensitive personal information for purposes of cross-context behavioral advertising.

Categories of Sources of Personal Information

In the past 12 months, we have collected personal information relating to Employee Personnel who are California residents from the following online and offline sources:

Categories of Sources of Personal Information	**Examples**
You	Information submitted on a job application, benefit enrollment forms, while performing job duties, in response to surveys or other requests for information
Service Providers	Benefit providers, software providers, communication services, fraud prevention services, data providers, data analytics providers
Affiliates	Information shared between companies under common ownership or control to Green Dot
Third parties authorized by you or directed to share information with Green Dot	Authorized agents, federal or state agencies, or others

PURPOSES FOR USE OF PERSONAL INFORMATION

We may use personal information relating to Employee Personnel who are California residents for any of the following purposes:

- Evaluating employment applications and employee job performance;
- Conducting background checks;
- Providing, maintaining, and improving Employee Personnel related services;
- Maintaining our facilities, systems, and infrastructure;
- Creating aggregated and de-identified information;
- For legal and business purposes, such as complying with federal, state, or local laws, responding to civil, criminal or regulatory lawsuits, subpoenas, or investigations, exercising our rights or defending against legal claims, resolving complaints and disputes, performing compliance activities, performing institutional risk control, and otherwise operating, managing and maintaining business operations;

- To comply with legal process, such as warrants, subpoenas, court orders, and lawful regulatory or law enforcement requests and to comply with applicable legal requirements;
- To protect and secure our websites, mobile applications, products, services, assets, network, and business operations, and to detect, investigate, and prevent activities that may violate our policies or be fraudulent or illegal;
- Debugging to identify and repair errors that impair existing intended functionality;
- Auditing related to Employee Personnel;
- Performing services on behalf of Green Dot or its service providers, including maintaining or servicing Employee Personnel accounts, providing services to Employee Personnel, processing or fulfilling orders and transactions, verification of Employee Personnel information, processing payments, providing financing, providing analytic services; and
- As described to you at the point of collecting your personal information.

CCPA RIGHTS AND REQUESTS

Please note that CCPA does not apply to certain information, such as information subject to the Health Insurance Portability and Accountability Act ("***HIPAA***"), the Fair Credit Reporting Act ("***FCRA***"), and other state or federal privacy laws.

As a California resident, you have the rights listed below. However, these rights are not absolute and in certain cases we may deny your requests as permitted by law. For example, we may deny your request if we cannot verify your identity or confirm that the personal information that we maintain relates to you, or if we cannot verify that you have the authority to make a request on behalf of another individual. In other instances, we may deny your request where an exception applies, such as where the disclosure of personal information would adversely affect the rights and freedoms of another individual or where the personal information that we maintain about you is not subject to the CCPA. You have the right to be free from unlawful discrimination or retaliation for exercising your rights under the CCPA.

If you are a California resident, you (or your authorized agent) may make the following requests:

(1) Request to Know (Access)

You may request that we disclose to you the following information covering the 12 months preceding your request:

- The categories of personal information we collected about you;
- The specific pieces of personal information we collected about you.

(2) Request to Delete

You may request that we delete personal information we collected from you. Once your personal information is deleted, we won't be able to get it back for you. If required by law, we will grant a request to delete information, but you should note that in many situations we must keep your personal information to comply with our legal obligations, resolve disputes, enforce our agreements, or for other business purposes.

(3) Request to Correct

You may request that we correct personal information about you that is no longer accurate or that is incorrect. In addition to submitting a Request to Correct, you may login to your Workday account to update your personal information located in your Workday account.

Submitting CCPA Requests

To exercise the CCPA rights described above, please submit a request by clicking here or calling us at 833-937-0515. In an effort to protect your personal information from unauthorized access, deletion or correction and/or to prevent fraud or theft of your personal information and any of your assets, we will verify and respond to your request consistent with applicable law, taking into account the type and sensitivity of the personal information subject to the request. Upon receiving a request, we will attempt to verify your identity by comparing the identifying information you provide with your request (e.g., your name and mailing address) to the personal information already maintained in our records. We may need to request additional personal information from you, such as your email address or telephone number, in order to verify your identity and protect against fraudulent requests. If you maintain a password-protected account with us, we may verify your identity through our existing authentication practices for your account and require you to re-authenticate yourself before disclosing or deleting your personal information. If you make a request to delete or correct, we may ask you to confirm your request before we delete or correct your personal information.
If we are subsequently unable to confirm your identity, we may refuse your rights request. We will not use personal information we collect in connection with verifying or responding to your request for any purpose other than responding to your request.

Authorized Agents

If you want to make a request as an authorized agent on behalf of an Employee Personnel that is a California resident, you may make a Request to Know, Request to Delete, or Request to Correct by clicking here or calling us at 833-937-0515. As part of our verification process, we may request that you provide:

- A power of attorney from the California resident pursuant to Probate Code sections 4121- 4130; or

- A completed Authorized Agent Designation Form signed by the California resident that you are submitting a request on behalf of a resident. Green Dot will provide you with a copy of this form for completion after you have submitted the request.

If the authorized agent does not provide documentation showing that the authorized agent has power of attorney to act on the resident's behalf, then the resident will also be required to independently verify their own identity directly with us and directly confirm that the resident provided the authorized agent permission to submit the rights request on their behalf.

DATA SECURITY

We have taken reasonable physical, administrative, and technical steps to safeguard the information we collect from and about our customers. While we make every effort to help ensure the integrity and security of our network and systems, we cannot guarantee our security measures. In the event that we are required by law to inform you of a breach to your personal

information we may notify you electronically, in writing, or by telephone, if permitted to do so by law.

ACCESS TO YOUR PERSONAL INFORMATION

You may sign in to your Workday account to access and/or update your personal information stored by us.

DATA RETENTION

We may store information about you for as long as we have a legitimate business need for it. We determine the retention period for each of the categories of personal information listed above based on (1) the length of time we need to retain the information to achieve the business or commercial purpose for which it was obtained, (2) any legal or regulatory requirements applicable to such information, (3) internal operational needs, and (4) any need for the information based on any actual or anticipated investigation or litigation.

CONTACT US

If you have any questions about this Employee CCPA Privacy Statement or the practices described herein, or if you need to access this Employee CCPA Privacy Statement in an alternative format due to having a disability, please contact us at the appropriate address below.

Mail: Green Dot Customer Service, P.O. Box 1070, Westchester, Ohio 45071-1070.
Phone: 833-937-0515

REVISIONS TO THIS STATEMENT

We reserve the right, at our sole discretion, to change, modify, add, remove, or otherwise revise portions of this Employee CCPA Privacy Statement at any time. When we do, we will post the change(s) on our websites and mobile applications.