

Ebara Technologies Inc. HR Privacy Notice

Effective Date: August 1, 2024

This Notice describes how we collect, use, process, and disclose personal information (“PI”) in various human resources (“HR”) contexts. References to “we,” “us,” “our,” and “Ebara” refer to Ebara Technologies Incorporated.

Applicability: This Notice applies to the California residents whose PI is collected in HR contexts, such as the following:

- Job applicants who have applied for a position with Ebara.
- Current/former employees of Ebara.
- Independent contractors of Ebara.

This Notice also applies to California residents whose family member or friend has provided PI about you to Ebara in an HR context, such as if:

- You are listed as an emergency contact for someone on the above list.
- You are a beneficiary or dependent of one of the foregoing.

Section 1 of this Notice provides notice of our data practices, including our collection, use, retention, and disclosure of PI. Section 2 applies only to California residents; it provides information regarding privacy rights under the CCPA and how California residents may exercise them. This Notice is designed to provide notice of our recent, historical data practices over the prior 12 months (from the Effective Date listed at the top of this Notice). *This Notice also applies to our current data practices, such that it is also meant to provide you with “Notice at Collection,”* which is notice of PI we collect online and offline, and the purposes for which we process personal information. For any new or substantially different processing activities that are not described in this Notice, we will notify you as required by applicable law, including by either notifying you at the time of collecting personal information, or by updating this Notice.

Amending this Notice. We reserve the right to amend this Notice at our discretion and at any time. When we make changes to this Notice, we will notice to you if required by applicable law.

Scope of Policy/Exclusions. Notably, this Notice does not apply to data that is not treated as PI under the CCPA or to the extent the data is subject to an exemption under applicable law. This Notice also does not apply to our online services such as our websites or our data practices outside of the HR context, which are addressed in our general privacy notice available [here](#).

You can click on the following blue links to navigate to the different sections in this Notice.

Table of Contents

1. [PI COLLECTION, USE, AND DISCLOSURES](#)
 - A. [COLLECTION AND DISCLOSURE DETAILS](#)
 - B. [SOURCES OF PI](#)
 - C. [DATA RETENTION](#)
2. [CONSUMER RIGHTS REQUESTS](#)

- A. [MAKING A REQUEST AND SCOPE OF REQUESTS](#)
- B. [VERIFYING YOUR REQUEST](#)
- C. [AUTHORIZING AN AGENT](#)
- D. [YOUR CONSUMER PRIVACY RIGHTS](#)
 - i. [RIGHT TO LIMIT SENSITIVE PI PROCESSING](#)
 - ii. [RIGHT TO KNOW/ACCESS](#)
 - a. [RIGHT TO KNOW CATEGORIES](#)
 - b. [RIGHT TO KNOW SPECIFIC PIECES](#)
 - iii. [RIGHT TO DELETE](#)
 - iv. [RIGHT TO CORRECT](#)
 - v. [DO NOT SELL/SHARE](#)
 - vi. [AUTOMATED DECISION-MAKING AND PROFILING](#)
 - vii. [RIGHT TO NON-DISCRIMINATION; NOTICE OF FINANCIAL INCENTIVE](#)

3. [CONTACT US](#)

1. *PI COLLECTION, USE, AND DISCLOSURES*

Generally, we collect, retain, use, and disclose your PI in order to provide you services and as otherwise related to the operation of our business, which include both business purposes and commercial purposes such as:

- Recruitment
- Intake/ Onboarding/ Offboarding
- Payroll, Reimbursements, and Timekeeping
- Benefits
- Employee activation initiatives
- Training programs and education
- HR IT Systems and Security
- Employee and Performance Management
- Health & Safety/Occupational Health
- Communicating with you
- Security (including electronic and data/information security and security of physical premises)
- The purposes explained at the time of collection (such as in the applicable privacy policy or notice).
- Other purposes that are related to or compatible with the context in which we collected your PI, or that are required or permitted by applicable law

Our business purposes also include the disclosure of PI (which may include all of the categories of PI in the tables below) to certain recipients, such as:

- Our vendors that perform services for us (including “Service Providers” and “Processors” defined under applicable laws, which we refer to as “Service Providers” herein) (“**Vendors**”).
- You or other parties at your direction or through your intentional action or consent.
- The government or private parties to comply with law or legal process.

- Assignees as part of an acquisition, merger, asset sale, or other transaction where another party assumes control over all or part of our business (“**Corporate Transaction**”), or to applicable parties in connection with or during negotiations related to a Corporate Transaction.
- In addition, our Vendors and other recipients listed in the below table may, subject to contractual restrictions imposed by us and/or legal obligations, also use and disclose your PI for business purposes. For example, our Vendors and the other categories listed in the table below may themselves engage Service Providers or subcontractors to enable them to perform services for us or process for our business purposes.

The table immediately below describes our data collection and disclosure practices in the HR context in further detail. In the table we describe the categories of PI we collect (left column), examples of types of data that fit within such categories (middle column), and the categories of recipients that receive such PI as part of disclosures for business purposes.

A. COLLECTION AND DISCLOSURE DETAILS

| Category of PI | Examples of types of PI within category | Categories of Recipients |
|--|--|--|
| 1. Identifiers and contact information | Name, alias, postal address, phone number, email address, driver’s license, social security number, employee ID, IP address and other online IDs. | <p>Disclosures for Business Purposes:</p> <ul style="list-style-type: none"> • Business Vendors • HR system and software vendors • Non-software HR vendors, such as background check vendors • Payroll and benefits vendors and providers • Insurance providers and brokers • Affiliates and related entities <p>Sale/Share: Information collected by Third-Party Digital Businesses on certain job applicant web pages may constitute a Sale/Share. See DO NOT SELL/SHARE section below.</p> |
| 2. Personal Records | Some PI included in this category may overlap with other categories. Examples include name, signature, social security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, education, | <p>Disclosures for Business Purposes:</p> <ul style="list-style-type: none"> • Business Vendors • HR system and software vendors • Non-software HR vendors, such as background check vendors • Payroll and benefits vendors and providers • Insurance providers and brokers • Affiliates and related entities <p>Sale/Share: N/A</p> |

| Category of PI | Examples of types of PI within category | Categories of Recipients |
|---|---|--|
| | employment, or employment history. | |
| 3. Personal Characteristics or Traits | In some circumstances, we may collect PI that is considered protected under applicable law, such as age, gender, nationality, race or information related to medical conditions. | <p>Disclosures for Business Purposes:</p> <ul style="list-style-type: none"> • Business Vendors • HR system and software vendors • Non-software HR vendors, such as background check vendors • Payroll and benefits vendors and providers • Insurance providers and brokers • Affiliates and related entities <p>Sale/Share: N/A</p> |
| 4. Commercial Information | Records of products or services purchased or obtained in the HR context, such as benefits you have signed up for. | <p>Disclosures for Business Purposes:</p> <ul style="list-style-type: none"> • Business Vendors • HR system and software vendors • Non-software HR vendors, such as background check vendors • Payroll and benefits vendors and providers • Insurance providers and brokers • Affiliates and related entities <p>Sale/Share: N/A</p> |
| 5. Internet and Service Usage Information | When you use our online systems or otherwise interact with us online or otherwise communicate with us, we may collect information regarding such use, interactions, or communications with us, our systems, and third-party applications, or other sites, applications, or content, subject to any applicable consent requirement. This includes information such as: your device functionality (browser, operating system, hardware, mobile network information); the URL that referred you to our service; the areas within our services and systems that you visit and | <p>Disclosures for Business Purposes:</p> <ul style="list-style-type: none"> • Business Vendors • HR system and software vendors • Affiliates and related entities <p>Sale/Share: Information collected by Third-Party Digital Businesses on certain job applicant web pages may constitute a Sale/Share. See DO NOT SELL/SHARE section below.</p> |

| Category of PI | Examples of types of PI within category | Categories of Recipients |
|--|--|--|
| | your activities there (such as browsing history and search history); your interaction with emails and messages we send you, such as whether you open them or click on links within; your device location (if you have enabled such features on your device); your device characteristics; and device data and the time of day. | |
| 6. Geolocation Data | If you use our systems or interact with us online we may gain access to the approximate or precise location of the device or equipment you are using, or the location from which you are accessing our systems. | <p>Disclosures for Business Purposes:</p> <ul style="list-style-type: none"> • Business Vendors • HR system and software vendors • Affiliates and related entities <p>Sale/Share: N/A</p> |
| 7. Audio, electronic, visual, thermal, olfactory, or similar Information | Examples of this category may include CCTV footage that we collect in our offices and facilities. | <p>Disclosures for Business Purposes:</p> <ul style="list-style-type: none"> • Business Vendors • HR system and software vendors • Affiliates and related entities <p>Sale/Share: N/A</p> |
| 8. Professional or Employment Information | For example, if you are an applicant, your current and prior jobs and education. If you are an employee, examples include your status of employment, title, performance reviews, and tenure. | <p>Disclosures for Business Purposes:</p> <ul style="list-style-type: none"> • General IT, software, and other business vendors • HR system and software vendors • Non-software HR vendors, such as background check vendors • Payroll and benefits vendors and providers • Insurance providers and brokers • Affiliates and related entities <p>Sale/Share: N/A</p> |
| 9. Non-public Education Records | For example, official grades, transcripts, class lists, or disciplinary records from your educational institution, may | <p>Disclosures for Business Purposes:</p> <ul style="list-style-type: none"> • Business Vendors • HR system and software vendors • Non-software HR vendors, such as background check vendors |

| Category of PI | Examples of types of PI within category | Categories of Recipients |
|----------------------------------|---|---|
| | be collected in the job application context. | <ul style="list-style-type: none"> • Affiliates and related entities Sale/Share: N/A |
| 10. Inferences from PI Collected | We may draw inferences from other information we collect about you. For example, based on your employment history, we may determine that your experience aligns with a job description. If you are an employee, we make inferences about your abilities and aptitude based on your job performance. | Disclosures for Business Purposes: <ul style="list-style-type: none"> • Business Vendors • HR system and software vendors • Payroll and benefits vendors and providers • Insurance providers and brokers • Affiliates and related entities Sale/Share: N/A |
| 11. Sensitive PI | <ul style="list-style-type: none"> • We collect the following categories of Sensitive PI: (a) Social Security, driver’s license, state identification card, or passport number; (b) account log-in in combination with any required security or access code, password, or credentials allowing access to an account; (c) communication content (e.g., the contents of a consumer’s mail, email, and text messages, other than where Ebara is the intended recipient of the communication); (d) precise geolocation; Health Information (PI collected and analyzed concerning a consumer’s health, medical history, | Disclosures for Business Purposes: <ul style="list-style-type: none"> • Business Vendors • HR system and software vendors • Affiliates and related entities Sale/Share: N/A |

| Category of PI | Examples of types of PI within category | Categories of Recipients |
|----------------|---|--------------------------|
| | mental or physical health, diagnosis/condition, and medical treatment). (e) Sensitive Personal Characteristics (e.g., racial or ethnic origin, religious or philosophical beliefs, citizenship or immigration status, or union membership). (f) Biometric Data (g) Children’s Data (PI collected from a known child) | |

B. SOURCES OF PI

We collect PI directly from you or from your Device, third parties (e.g., background check and vendors, references, job agencies), including public sources of data, Vendors, our affiliates and related entities, and other third parties. In addition, if you are an emergency contact, beneficiary, or dependent, we may collect PI about you from your family member or friend who is employed by us.

C. DATA RETENTION

Because there are so many different types of PI in each category, and so many purposes and use cases for different data, we are unable to provide retention ranges based on categories of PI in a way that would be meaningful and transparent to you. Retention periods for each category of PI will depend upon how long we have a legitimate purpose for the retention consistent with the collection purposes and applicable law. For instance, we may maintain business records for so long as relevant to our business, and may have a legal obligation to hold PI for so long as potentially relevant to prospective or actual litigation or government investigation. We apply the same criteria for determining if we have a legitimate purpose for retaining your PI that you ask us to delete. If you make a deletion request, we will conduct a review of your PI to confirm if legitimate ongoing retention purposes exist, will limit the retention period to such purposes for so long as the purpose continues, and will respond to you with information on any retention purposes on which we rely for not deleting your PI. For more information on deletion requests, see the [Right to Delete](#) section.

2. CONSUMER RIGHTS REQUESTS

As described in further detail below, subject to meeting the requirements for a Verifiable Request (defined below), we provide the privacy rights to California residents whose PI we have collected in an HR context as described in this section.

A. MAKING A REQUEST AND SCOPE OF REQUESTS

As permitted by the CCPA, any request you submit to us is subject to an identity verification process (“**Verifiable Request**”) as described below in the “[Verifying Your Request](#)” section below. We will not fulfill your request unless you have provided sufficient information for us to reasonably verify you are the individual about whom we collected PI.

To make a request, please submit your request to us by one of the methods below:

- Calling us at 1-888-416-3414
- Using our Contact Us form at <https://www.ebaratech.com/about-ebara/contact-us/>.
- For current employees, you can also contact your HR representative

Some PI we maintain about an individual is not sufficiently associated with enough PI about the individual for us to be able to verify that it is a particular individual’s PI. We do not include that PI in response to those requests. If we cannot comply with a request, we will explain the reasons in our response.

You are not required to create a password-protected account with us to make a Verifiable Request. We will use PI provided in a Verifiable Request only to verify your identity or authority to make the request and to track and document request responses, unless you also gave it to us for another purpose.

We will make commercially reasonable efforts to identify PI that we collect, process, store, disclose, and otherwise use and to respond to your privacy requests. We will typically not charge a fee to fully respond to your requests; provided, however, that we may charge a reasonable fee, or refuse to act upon a request, if your request is excessive, repetitive, unfounded, or overly burdensome. If we determine that the request warrants a fee, or that we may refuse it, we will give you notice explaining why we made that decision. You will be provided a cost estimate and the opportunity to accept such fees before we will charge you for responding to your request.

B. VERIFYING YOUR REQUEST

When you make a request, we will verify that you are the person you say you are, or, if you are seeking information on behalf of another person, that you are authorized to make the request on their behalf. In addition, we will compare the information you have provided to ensure that we maintain personal information about you in our systems. We ask that you provide us with, at a minimum, your full name and phone number and/or email. Depending on the nature of the request and whether we have the phone number or email address you have provided in our systems, we will request further information from you in order to verify that you are the individual about whom we have collected information. We will review the information provided as part of your request, and may ask you to provide additional information via e-mail or other means as part of this verification process. We will not fulfill your Right to Know (Categories), Right to Know (Specific Pieces), Right to Delete, or Right to Correction request unless you have provided sufficient information for us to reasonably verify you are the individual about whom we collected PI. The same verification process does not apply to opt-outs of Sale or Sharing, or limitation of Sensitive PI requests, but we may apply some verification measures if we suspect fraud.

The verification standards we are required to apply for each type of request vary. We verify your categories requests and certain deletion and correction requests (e.g., those that are less sensitive in nature) to a reasonable degree of certainty, which may include matching at least two data points provided by you with data points maintained by us, which we have determined to be reliable for the purpose of verifying you. For certain deletion and correction requests (such as those that relate to personal information that is more sensitive in nature) and for specific pieces requests, we apply a verification standard of reasonably high degree of certainty. This standard includes matching at least three data points provided by you with data points maintained by us, which we have determined to be reliable for the purpose of verifying you, and may include obtaining a signed declaration from you, under penalty of perjury, that you are the individual whose personal information is the subject of the request.

If we cannot verify you with respect to certain requests, such as if you do not provide the requested information, we will still take certain action as required by the CCPA. For example:

- If we cannot verify your deletion request, we will refer you to this Notice for a general description of our data practices.
- If we cannot verify your specific pieces request, we will treat it as a categories request.

C. AUTHORIZING AN AGENT

You may designate an authorized agent to submit your request on your behalf by submitting a request in the manners described above. If you are an authorized agent who would like to make a request, the CCPA requires that we ensure that a request made by an agent is a Verifiable Request (except Do Not Sell/Share requests) and allows us to request further information to ensure that agent is authorized to make the request on an individual's behalf. Generally, we will request that an agent provide proof that the subject of the request gave the agent signed permission to submit the request, and, as permitted under the CCPA, we also may require that individual whose PI is subject to the request to either verify their own identity or directly confirm with us that they provided the agent permission to submit the request.

D. YOUR CONSUMER PRIVACY RIGHTS

i. RIGHT TO LIMIT SENSITIVE PI PROCESSING

Certain personal information qualifies as Sensitive PI under the CCPA, which we refer to in this Notice as "**Sensitive PI.**" The CCPA provides the right to direct businesses to limit their use and disclosure of Sensitive PI if we use or disclose it beyond certain internal business purposes. However, we do not use or disclose Sensitive PI beyond such internal business purposes.

ii. RIGHT TO KNOW/ACCESS

a. RIGHT TO KNOW CATEGORIES

If you are a California resident, you have the right to request that we share with you certain information about our collection, use, and disclosure of your PI over the 12-month period prior to the request date, related to categories of PI. You can request that we disclose to you: (1) the categories of PI we collected about you; (2) the categories of sources for the PI; (3) our business or commercial purpose for collecting, selling, or sharing that PI (i.e., if we have, in fact, sold PI); (4) the categories of third parties with whom we

disclosed that PI to; (5) a list of the categories of PI disclosed for a business purpose in the prior 12 months and, for each, the categories of recipients, or that no disclosure occurred; and (6) a list of the categories of PI sold or shared about you in the prior 12 months and, for each, the categories of recipients, or that no sale or share occurred.

b. RIGHT TO KNOW SPECIFIC PIECES

You have the right to request a transportable copy of the specific pieces of PI we collected about you on or after the CCPA's lookback date, which is January 1, 2022. Please note that PI is retained by us for various time periods, so there may be certain information that we have collected about you since the lookback date, but that we no longer retain; there also may be PI collected 12 months prior to your request that proves impossible to provide or that would involve disproportionate effort to provide (and thus, it would not be able to be included in our response to you). Please also note that you are limited to making two "right to know" requests in any 12-month period.

iii. RIGHT TO DELETE

You have the right to request that we delete any of your PI that we have collected directly from you and retained, subject to certain exceptions which we will explain if they apply. After we confirm that your deletion request is a Verifiable Request, subject to permitted retention exemptions, we will carry out one or more of the following: (i) permanently erase your PI on our existing systems with the exception of archived or back-up systems; (ii) deidentify your PI; or (iii) aggregate your PI with other information. In our response to your request to delete, we will tell you the method for deleting your PI. Where legal exceptions will apply to your request for deletion, we will tell you which one(s) and will limit retention to the permitted purpose(s).

iv. RIGHT TO CORRECT

You have the right to request that we correct inaccuracies that you find in your PI maintained by us. Your request to correct is subject to our verification (discussed above) and the response standards set forth in the CCPA.

v. DO NOT SELL/SHARE

Under the CCPA, you have the right to opt-out of certain processing activities. California has opt-outs specific to targeted advertising activities – which the CCPA refers to as “cross-context behavioral advertising” – and which involves the use of PI from different businesses or services to target advertisements to you. The CCPA provides the right to opt-out of Sharing, which includes providing or making available PI to third parties for such targeted advertising activities. The CCPA also has opt-outs specific to the Sale of PI, which at a minimum requires providing or otherwise making PI available to a third party.

Third-Party digital businesses (“Third-Party Digital Businesses”) may collect information about your device and/or your visit to webpages that you visit while applying for a position with Ebara, through cookies and other tracking technologies. Giving access to PI on the Service, or otherwise, to Third-Party Digital Businesses for the business and commercial purposes of advertising (for recruiting purposes) and analytics could be deemed a Sale and/or Sharing. Therefore, we will treat such PI collected by Third-Party Digital Businesses (e.g., cookie ID, IP address, and other online IDs and internet or other electronic activity

information) as such, and subject to the opt-out requests described above. In some instances, the PI we make available about you is collected directly by such Third-Party Digital Businesses using cookies and other tracking technologies on the Service or our advertisements that are served on third-party sites (which we refer to as “cookie PI”). If you would like to submit a request to opt-out of our processing of your cookie-related PI relating to the Sale or Sharing of such data, you need to exercise a opt-out request on our cookie management tool [here](#). Our cookie management tool enables you to exercise such an opt-out request and enable certain cookie preferences on your device. You must exercise your preferences on each of our websites you visit, from each browser you use, and on each device that you use. Since your browser opt-out is designated by a cookie, if you clear or block cookies, your preferences will no longer be effective, and you will need to enable them again via our cookie management tool.

The CCPA also requires us to state that we do not knowingly Sell or Share the PI of California residents under 16.

We may disclose your PI for the following purposes, which are not a Sale or Sharing: (i) if you direct us to share your PI; (ii) to comply with your requests under the CCPA; (iii) disclosures amongst the entities that constitute Ebara as defined above, to Ebara’s service providers, or as part of a Corporate Transaction; and (iv) as otherwise required or permitted by applicable law.

vi. AUTOMATED DECISION-MAKING AND PROFILING

We do not believe we engage in processing that constitutes automated decision-making or profiling under the CCPA. The CCPA regulations that cover these concepts have not yet been finalized as of the date of this Notice. If necessary, we will update this Notice to address any requirements in these areas when the regulations are finalized.

vii. RIGHT TO NON-DISCRIMINATION; NOTICE OF FINANCIAL INCENTIVE

We will not discriminate against you in a manner prohibited by the CCPA because you exercise your privacy rights. We do not currently offer discounts or rewards for providing us PI, or set price or service differences related to the collection, retention, Sale, or Sharing of PI. If we offer such programs in the future, we will update this Notice to describe such program(s), including how you may opt-in and how we value the PI required.

3. CONTACT US

If you have any questions about the Notice or practices described in it, you should contact us in the following ways: Postal Mail: 51 Main Avenue Sacramento CA 95838, Attn: Human Resources; Email: Consumerprivacy@ebaratech.com. Current employees may also contact their HR representative.