

Inbenta Applicant Privacy Policy

Effective date: March 20, 2024

This Applicant Privacy Policy explains what personal data we collect from Job Applicants, how we use and share that information, and the rights and choices you have in connection with that information, including how you can limit certain uses and sharing of your information.

When we refer to “personal data,” we mean information about an identified individual or that would allow us to identify an individual. Subject to applicable law, personal data generally does not include publicly available information or anonymized or de-identified data. For more information about our privacy practices, contact us by email at privacy@inbenta.com.

TABLE OF CONTENTS

1. [Who You Are](#)
 - a. [Types of information we collect about Job Applicants and why](#)
 - b. [How we collect information about Job Applicants](#)
 - c. [Parties to whom we may disclose personal data about Job Applicants](#)
2. [Localization of Data Storage and Processing](#)
3. [Data Security](#)
4. [Additional Information for Job Applicants](#)
 - a. [Applicable Law](#)
 - b. [Contact](#)
 - c. [Privacy Rights](#)
 - d. [Data Retention](#)
5. [Updates to this Privacy Policy](#)

1. WHO YOU ARE

This Applicant Privacy Policy applies to all individuals who apply for employment at Inbenta, including while you are in a selection process, and our collection, use, or disclosure of these individuals' personal data until actual employment begins.

a. Types of personal data we collect about Job Applicants and why

We may collect the following categories of personal data about Job Applicants, for the purposes stated in the chart. Please note that the categories of data collected may vary between countries/states.

** For applicants residing in California, these categories of data correspond to data we may have collected in the proceeding 12 months.*

Category of Personal Data	Examples	Purpose of Collection and Use
Identifiers	First and last name, date of birth	<ul style="list-style-type: none"> • Process employment applications • Detect and prevent fraud • Comply with legal or regulatory obligations
Contact information	Personal email address, personal phone number, address	<ul style="list-style-type: none"> • Process employment applications • Communicate with Job Applicants
Professional or employment-related information	Background information such as professional experience, job titles, employment history, references, online professional profile, optional information on salary expectation	<ul style="list-style-type: none"> • Process employment applications • Make employment and compensation decisions • Detect and prevent fraud • Comply with legal or regulatory obligations
Education information	Educational institutions attended, dates of attendance, degrees granted	<ul style="list-style-type: none"> • Process employment applications • Make employment and compensation decisions
Inference information	Inferences about a job applicant's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes	<ul style="list-style-type: none"> • Process employment applications • Make employment and compensation decisions • Comply with applicable law
*Sensitive personal information	Social Security number	<ul style="list-style-type: none"> • Process employment applications • Comply with applicable law
*California Consumer Records law information	Name, social security number, address, telephone number, education, employment, employment history, medical information	<ul style="list-style-type: none"> • Process employment applications • Communicate with Job Applicants • Make employment and compensation decisions

		<ul style="list-style-type: none"> • Comply with applicable law
--	--	--

b. How we collect information about Job Applicants

We may collect personal data about Job Applicants from the following sources stated in the chart.

** For applicants residing in California, these categories of data correspond to data we may have collected in the proceeding 12 months.*

Sources of Personal Data	Categories of Personal Data We Collect
<p><i>Directly from you</i></p> <p>We may collect personal data from you when you interact with the Careers section at the Inbenta Site, managed by a third-party vendor, or LinkedIn, or in person.</p>	<ul style="list-style-type: none"> • Identifiers • Contact information • Professional or employment-related information • Inference information • *Sensitive personal information • *California Consumer Records Law information
<p><i>From third parties</i></p> <p>We may collect personal data about Job Applicants through other third parties, such as through reference calls during the hiring process or communicating with other entities to track and maintain appropriate records of education, training, and development activities, as necessary to make employment, and promotion decisions.</p>	<ul style="list-style-type: none"> • Identifiers • Professional or employment-related information • Education information • Inference information • *California Consumer Records law information

c. Parties to whom we may disclose information about Job Applicants

We disclose personal data about Job Applicants as stated in the chart.

We do not use or disclose sensitive personal information about Job Applicants for purposes other than to complete the personnel selection process; to prevent, detect, and investigate security incidents that compromise the availability, authenticity, integrity, or confidentiality of stored or transmitted personal data; to resist malicious, deceptive, fraudulent, or illegal actions directed at us and to prosecute those responsible for those actions.

** For applicants residing in California, these categories of data correspond to data we may have collected in the proceeding 12 months.*

Categories of Third-Party Recipient and Purpose for Disclosure	Categories of Personal Data We May Share
<p><i>Parents, Affiliates, and Subsidiaries</i></p> <p>Inbenta Holdings Inc. is the parent entity of our group of companies that make up the Inbenta family. We may disclose personal data about Job Applicants to other companies within the Inbenta family, in order to make employment decisions. When we disclose personal data about Job Applicants to other companies within the Inbenta family, their collection, use, and disclosure of that personal data is subject to this Policy.</p>	<ul style="list-style-type: none"> • Identifiers • Contact information • Professional or employment-related information • Education information • Inference information • *Sensitive personal information • *California Consumer Records law information
<p><i>Service providers</i></p>	<ul style="list-style-type: none"> • Identifiers

<p>We engage third-party service providers to perform a variety of services on our behalf, which may mean that we have to disclose personal data about Job Applicants to these third parties. When we disclose personal data in this way, we put in place appropriate measures to make sure that our service providers keep the personal data confidential and secure.</p>	<ul style="list-style-type: none"> ● Contact information ● Professional or employment-related information ● Education information ● Inference information ● *Sensitive personal information ● *California Consumer Records law information
<p><i>Professional Services Firms</i></p> <p>We may disclose personal data about Job Applicants to professional services firms that help us comply with our legal and regulatory obligations and establish, enforce, and otherwise exercise our rights and defend against claims, including, for example, auditors, law firms, and consultants.</p>	<ul style="list-style-type: none"> ● Identifiers ● Contact information ● Professional or employment-related information ● Education information ● Inference information ● *Sensitive personal information ● *California Consumer Records law information
<p><i>Government entities</i></p> <p>We may disclose personal data to government entities and agencies, regulators, law enforcement, and other third parties, including to comply with applicable laws and regulations, to respond to a subpoena, search warrant, or pursuant to legal process, and to establish or exercise our legal rights or for fraud or crime-prevention purposes or for the protection of the rights, property, or safety of our company or third parties.</p> <p>We may also disclose personal data in relation to a known or suspected violation of our terms of use, fraud prevention or other unlawful use, including with entities assisting us with an investigation, or as may be required by applicable law.</p> <p>We may also disclose personal data to confirm or verify a California resident's right to work in the United States.</p>	<ul style="list-style-type: none"> ● Identifiers ● Contact information ● Professional or employment-related information ● Education information ● Inference information ● *Sensitive personal information ● *California Consumer Records law information
<p><i>Merger and Acquisition Activity (Successor organizations)</i></p> <p>As may be relevant to the underlying transaction, we may disclose personal data about Job Applicants to third parties in connection with the proposed or actual financing, insuring, sale, securitization, assignment, or other disposal of all or part of our business or assets (including accounts) for the purposes of evaluating and performing the proposed transaction.</p>	<ul style="list-style-type: none"> ● Identifiers ● Contact information ● Professional or employment-related information ● Education information ● Inference information ● *Sensitive personal information ● *California Consumer Records law information

2. LOCALIZATION OF DATA STORAGE AND PROCESSING

The management of your job application may involve the processing of personal data by Inbenta affiliates located in different countries (resulting in international data transfers). However, it is only done in virtue of an

Intercompany Data Processing and Transfer Agreement which, when applicable, includes Standard Contractual Clauses (SCC) in accordance with the decision of the European Commission to data transfers from data exporters in the EU to data importers established outside the EU.

Specifically, information we collect from you might be processed in the United States, and by applying to a job opening at Inbenta, you acknowledge and consent to the processing of your data in the United States.

3. DATA SECURITY

We have taken steps to secure and protect your personal data from loss, unauthorized access, unauthorized disclosure, misuse, destruction, or alteration. However, there is always some risk involved in transmitting information over the Internet, and we cannot fully eliminate security risks associated with the storage and transmission of personal data.

4. ADDITIONAL INFORMATION FOR JOB APPLICANTS

a. Applicable law

We process your personal data (i) based upon your consent, as necessary for the management of your job application, (ii) based on legitimate interests, or (iii) as required by our legal obligations.

Inbenta does not use or disclose sensitive personal data other than to prevent, detect, and investigate security incidents or to resist malicious, deceptive, fraudulent, or illegal actions, or as required by law.

EEA: The General Data Protection Regulation (GDPR) governs processing of personal data by organizations in the European Economic Area or about individuals located in the European Economic Area. The current members of the European Economic Area are Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, and Sweden.

UK: The UK GDPR governs processing of personal data by organizations in the United Kingdom or about individuals located in the United Kingdom.

Brazil: The Lei Geral de Proteção de Dados (LGPD) regulates the collection, use, and disclosure of personal data of individuals in Brazil and by companies located in Brazil. If we are processing your personal data in Brazil, the controller of your data is Inbenta Brasil Consultoria E Tecnologia LTDA.

California (U.S.): The California Consumer Privacy Act (CCPA), as amended by the California Privacy Rights Act, gives California residents enhanced rights with respect to their personal data that is collected by businesses. This section explains what rights California residents may have under the CCPA.

Japan: The Act on the Protection of Personal Information regulates the collection, use, and disclosure of personal data by organizations in Japan. The personal information handling business operator in Japan is Inbenta Japan LLC.

b. Contact

Inbenta may be contacted as follows:

Data Controller and Parent entity: Inbenta Technologies Inc. 950 West Bethany Drive, Suite 400	Representative in Europe: Inbenta Holdings Inc. Spain Branch Aribau 64 BJ, 08011 Barcelona, Spain
--	---

Allen, TX 75013 USA	
<p>Brazil:</p> <p>Inbenta Brasil Consultoria E Tecnologia LTDA Av. Paulista, 2028 – 10º andar – Bela Vista São Paulo - SP - 01310-200</p>	<p>Japan:</p> <p>Inbenta Japan LLC T010-0966 Akita-ken Akita-shi Sanno 1-10-22 Ishikawa Jumusho - Bill 1F A</p>

For more information about our privacy practices, or to exercise your privacy rights, contact us by email at privacy@inbenta.com.

For EEA inquiries, contact our Data Protection Officer by email at dpo@inbenta.com or at the following address:
Aribau 64 BJ, 08011 Barcelona, Spain

c. Privacy Rights

As a Job Applicant, you may have the following privacy rights. Please note that these rights may vary between counties/states, are not absolute, and may be subject to change, limitations, or restrictions. For example, we may decline to provide you with access to your personal data if doing so would be likely to harm the life, body, property, or other rights or interests of you or someone else or would be likely to seriously interfere with the proper implementation of our businesses. If we decline to do what you have requested in full or in part, we will strive to explain the reason why to you.

- Right to Access: You have the right to request access to your personal data held by Inbenta and obtain information about how it is being processed.
- Right to Rectification: You can request the correction of inaccurate or incomplete personal data.
- Right to Erasure (Right to Be Forgotten): You have the right to request the deletion or removal of your personal data under certain circumstances.
- Right to Restrict Processing: You can request the limitation of processing your personal data under specific conditions.
- Right to Data Portability: You can request your personal data to be provided in a structured, commonly used, and machine-readable format or transferred to another organization.
- Right to Object: You can object to the processing of your personal data, including direct marketing and certain automated processing.
- Right to Withdraw Consent: You have the right to withdraw your consent for processing personal data where consent is the lawful basis for processing.
- Right to Non-Discrimination: You have the right not to be discriminated against for exercising your privacy rights.
- Right to Opt-Out: You have the right to opt-out of the sale* of your personal data under certain regulations such as CCPA.
- Right to Information (Right to Know): You have the right to be informed about how your personal data is being processed, the purpose, and the recipients of your data.
- Right to File a Complaint: Individuals have the right to lodge a complaint with a relevant data protection authority regarding the processing of their personal data.
 - If you are in the European Economic Area or would like to contact a European supervisory authority, their contact information is [here](#).
 - If you are in the United Kingdom or would like to contact the UK Information Commissioner's Office, you can do so [here](#).
 - If you are in Brazil, you can lodge a complaint with the [Autoridade Nacional de Proteção de Dados \(ANPD\)](#), or with the Consumer's rights authorities (PROCON) of your Brazilian state of residence.

**The CCPA defines "sale" to include data transfers for monetary or other valuable consideration. We do not sell or share your personal information to third parties based on the CCPA definitions of "sell" and "share". As*

stated above in the data collection sections, we collect and transmit your data to third-party service providers in order to manage your employment relationship.

You may exercise your privacy rights by the communication means mentioned in the < [Contact](#) > section.

If you email us, please put in the subject line of your email the right you are seeking to invoke: For example, "Applicant Right to Erasure" or "Applicant Right to Object".

We will confirm receipt of your request to know, delete, or correct within 10 days along with a description of what steps we will take to verify and respond. We must provide the requested information or delete your personal data within 45 days of receipt of your request but can use an additional 45 days, but we will let you know if additional time is needed.

When contacting us, we may ask you to provide certain, limited personal data, such as your name, e-mail address and/or username to verify your request and to match with our records and systems. We will not retain this personal data or use it for any other purpose.

d. Data Retention

We retain personal data for as long as needed or permitted in light of the purpose(s) for which it was obtained. The criteria used to determine our retention periods include:

- the length of time we have an ongoing relationship with you;
- whether there is a legal obligation to which we are subject; and
- whether retention is advisable in light of our legal position (such as in regard to applicable statutes of limitations, litigation or regulatory investigations).

5. UPDATES TO THIS PRIVACY POLICY

We may update this Applicant Privacy Policy from time to time. The "effective date" at the top of this privacy policy indicates when this privacy policy was last revised.

END OF DOCUMENT