Last Revised: June 2026

CANDIDATE PRIVACY POLICY

Verkada Inc., and its subsidiaries ("Verkada", "we", "our", or "us") are committed to protecting your privacy rights. This privacy policy (the "Candidate Privacy Policy") explains how we collect, use, protect and otherwise process your Personal Information throughout our recruitment process. Verkada Inc., and where relevant the local Verkada subsidiary or affiliate, will each be a controller of your Personal Information and is responsible for deciding how we process and store it.

In this Candidate Privacy Policy, Personal Information means information from which you may be identified directly (from that information alone) or indirectly (when different pieces of information are combined).

This Candidate Privacy Policy applies to job applicants only and does not apply to current Verkada employees. It also does not form part of any employment contract or contract to provide services. If you provide information to Verkada through or in connection with another company, we are not responsible for that company's privacy practices. This Candidate Privacy Policy does not apply to personal information processed when you use our business website, which is governed by our Privacy Policy.

What Personal Information We Collect

In connection with the recruitment process, we will collect, store and otherwise process Personal Information about you including:

- information you provided in your CV and accompanying letter, such as your name, contact details, education history, employment history and experience, photo, achievements, work authorization, visa status
- information regarding how you came to apply for the role
- information you provided on our application forms, including name, title, address, telephone number, personal email address, date of birth, gender, education history, employment history, qualifications, degrees or certifications
- our application forms may also request role-specific qualifications or experience information
- information from your professional social media account, such as LinkedIn profile

picture and contact details
- information relating to your background, including employment and address verification, bank account verification and criminal background checks (as relevant to the role and as appropriate)(see below for more information)
- information regarding visa status
- information collected during the reference check, vetting process, and the time of offer
- information you provide during an interview including, without limitation, audio or visual information we may collect as part of interviews or other meetings we conduct with you
- information collected as you progress through the recruitment process, such as how you learned about the vacant position, whether you are eligible to work abroad, which passports / visas / work authorizations you hold, any non-compete or non-solicitation obligations, any other areas of potential conflicts of interest
- your feedback if you choose to provide it

Depending on geography, subject to your consent and on an entirely voluntary basis, we may also collect, store and use other sensitive Personal Information about your race, ethnicity, veteran, criminal record, and disability status.

Cookies and Tracking Technologies

When you visit our Careers page or submit an application through our website, we may use cookies and similar tracking technologies in accordance with our Site Cookie Policy. For more information about how we use cookies and your choices, please review our Site Cookie Policy.

How Your Personal Information Is Collected

We may collect Personal Information about you from the following sources:

- yourself
- employees who may refer you for a role
- your current or former colleagues, references or other contacts in your professional network
- third parties, such as a publicly accessible source
- social media companies, such as LinkedIn
- third-party agents, such as recruiters
- third-party vendors who provide or assist with background checks

We may also use LinkedIn to actively search for profiles which we think would align to our job vacancies. Some information from your LinkedIn profile will be collected and processed by us if we interact with you through the LinkedIn channel. If we identify a profile that is interesting to us, we may message you directly on LinkedIn and invite you to interview for the vacant position. We may also use LinkedIn Recruiter, which allows us access to enhanced features to leverage LinkedIn's networks and reach more potential candidates. If we are already connected with you, we may obtain your contact information from your LinkedIn profile, if we are not already connected with you, you will be asked by LinkedIn if you'd like to share your contact information with us (voluntarily) when we reach out to you.

How We Use Your Personal Information

We may use your Personal Information to process your application, including to:

- assess your skills, qualifications and suitability for the role
- carry out checks from references, your professional network, colleagues from your current or former roles, background vetting (if required)
- communicate with you about the recruitment process
- keep records related to our hiring processes
- retain your information for future positions (unless you request that it be deleted)
- conduct internal audits and workplace investigations

- perform workforce and applicant pool analytics, data analytics and benchmarking
- evaluate your work authorization in the relevant geography
- review your application, resume, schedule interviews, and record and analyze the interview content using tools that leverage artificial intelligence, where permitted (these tools support human decision-making and do not make hiring decisions)
- improve Verkada's recruitment processes and services
- comply with legal or regulatory requirements

To aid our recruitment process, we may use third-party tools to help identify potential candidates who match certain objective role requirements (e.g., educational degrees, professional certifications, years of experience). For example, we may use platforms like LinkedIn to search for passive talent, where we supply the search criteria and review suggested profiles before deciding whether to reach out.

If we determine that you meet the basic requirements to be shortlisted for the role, we will invite you to interview for the role. If we decide to offer you the role, we will then take up reference, employment background and other checks before commencing employment. If you do not provide information necessary for us to consider your application (such as evidence of qualifications or work history), we may not be able to process your application.

We also may use information in an aggregated and/or de-identified way, including to monitor application and hiring trends within Verkada.

How We Use Sensitive Personal Information

We may use your Sensitive Personal Information (such as gender, race, national or ethnic origin, citizenship or immigration status, veteran or disability status or criminal record) for legitimate recruitment and employment purposes or to support you as a job applicant or employee of Verkada such as:

- to consider whether we need to provide appropriate adjustments or accommodations for you during the recruitment process
- for work authorization purposes
- for government reporting purposes (e.g. United States (U.S.) federal contractor and equal employment opportunity laws require that we ask candidates to volunteer information about their sex, race, ethnicity, veteran and disability status)
- to do equal opportunity monitoring and reporting (such information will be collected and stored in de-identified form)
- to comply with legal obligations

With the exception of work authorization information, you decide whether or not to provide such information–it's entirely voluntary. Your decision has no impact on our review of your application, and we do not make decisions about employment based on Sensitive Personal Information.

Pre-Employment Checks and Verifications

We work with a third-party vendor to carry out various checks and verifications after we have made an offer of employment, and if required, we will ask for your consent to do so. We will provide you with the name of the relevant third-party vendor and information about the process via email if your application progresses to the background phase. The vendor will reach out to you to complete your checks and then you will submit your information directly to the background vendor. Examples of verification and background checks we perform include:

- Criminal background checks
- Education verification checks (e.g., schools attended, subjects studied, dates of attendance)
- Employment verification checks (e.g., dates of employment, positions held)
- Vehicle report checks (e.g., class of licence, safety record, legal ability to drive)

(where relevant)
- Checks against a global watchlist

Which checks and verifications are carried out will depend on your location and the location of your role.

Where we rely on your consent for these checks and verifications, you can withdraw your consent at any time. If you do, we will be unable to carry out our background checks.

How We Disclose Your Personal Information

We may disclose your Personal Information to third parties or agents, including the following:

- other companies in our group and affiliates
- third parties or agents to assist in the administration, processing and management of certain activities pertaining to prospective employees
- applicant tracking systems to manage our application process
- individuals or companies employed by Verkada to carry out specific services, functions or consultancy work
- financial institutions
- relatives, references, colleagues, former colleagues or legal representatives of prospective employees
- regulatory bodies, government departments/agencies or courts as required;
- other parties with your consent and as permitted by law
- other vendors that support us in our recruitment processes

We may also disclose your Personal Information for legal compliance purposes and to exercise our legal rights, including (1) in response to a legitimate request for assistance by law enforcement, (2) to seek legal advice from our external lawyers, or (3) in connection with litigation or claims of litigation. We may also disclose your Personal Information in connection with the negotiations up to or the actual sale, purchase, or merger of our business.

Where Your Personal Information Is Stored and Processed

Your Personal Information may be transferred to, and processed in, countries other than the country in which you are a resident. These countries may have data protection laws that are different from the laws of your country (and, in some cases, may not be as protective), and data may be accessible to law enforcement and national security authorities under certain circumstances.

By providing your Personal Information to Verkada, you acknowledge the transfer of your information to the U.S. for storage, use, processing, maintenance, and onward transfer of such information to other entities, regardless of their location.

Vendors that we work with and our affiliated companies and subsidiaries within our corporate group may also process your Personal Information in the U.S. and / or facilitate the transfer of or access to your Personal Information outside of the U.S. We will take steps to require them to process your Personal Information subject to appropriate safeguards (e.g., implementing standard contractual clauses where appropriate).

Verkada currently relies on and complies with the EU-U.S. Data Privacy Framework, the UK Extension to the EU-U.S. Data Privacy Framework, and the Swiss-U.S. Data Privacy Framework ("Data Privacy Frameworks" or "DPF") as a legal basis for transfers of Personal Information from the EU, the UK, and Switzerland to the U.S in the context of the employment relationship, including Personal Information relating to employees, job applicants, and other members of Verkada's workforce. Verkada has certified to the Department of Commerce that we adhere to the Principles of the Data Privacy Frameworks ("Principles") and Verkada complies with its obligations under the Principles. Verkada adheres to the Principles for onward transfers of Personal Information to third

parties and remains liable for damages caused by third parties under the DPF unless Verkada is not responsible for the event giving rise to damage. The U.S. Federal Trade Commission has jurisdiction over Verkada's compliance with the DPF. To learn more about the Data Privacy Framework program, please visit https://www.dataprivacyframework.gov/, where you can view Verkada's certifications.

If we receive your Personal Information under the Data Privacy Framework, you can exercise certain choices regarding how some of your Personal Information is used and disclosed, as set forth in the "Rights and Choices" section below depending on where you reside.

In compliance with the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF, Verkada commits to cooperate with, and comply with the advice of, the relevant European Union supervisory authorities, the UK Information Commissioner's Office, and the Swiss Federal Data Protection and Information Commissioner with respect to complaints concerning Personal Information transferred under the DPF in the context of the employment relationship.

In compliance with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF, Verkada further commits to refer unresolved complaints concerning our handling of Personal Information received in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF to JAMS, an alternative dispute resolution provider based in the U.S. If you do not receive timely acknowledgment of your DPF Principles-related complaint from us, or if we have not addressed your DPF Principles-related complaint to your satisfaction, please visit the JAMS DPF Dispute Resolution webpage for more information or to file a complaint. The services of JAMS are provided at no cost to you. If neither Verkada nor our dispute resolution provider resolves your complaint, you may have the possibility to engage in binding arbitration through the Data Privacy Framework Panel. For more information on this option, please see Annex I of the EU-U.S.Data Privacy Framework Principles.

Data Security

We have put in place appropriate security measures to help prevent unauthorized access, loss or use of your Personal Information, but we cannot guarantee the security of your Personal Information. Employees, agents, contractors and other third parties who access Personal Information are subject to confidentiality obligations.

How Long We Keep Your Personal Information

If your application for employment or engagement is successful, Personal Information gathered during the recruitment process will be retained and additional information will be collected for use in our employee and HR information systems and retained in accordance with our employee privacy notices and employment policy.

If your application for employment or engagement is unsuccessful, we will hold your data on file for up to two (2) years (subject to any applicable legal or regulatory obligations to retain such information for a shorter or longer period or to defend or exercise legal claims) to consider you for future positions. You can write to us at any time and request that we no longer keep your information for this purpose by submitting a request through our online form or contacting us at 833.280.5900.

At the end of that period, we will securely destroy your Personal Information, unless otherwise permissible under applicable law or if we are required to maintain it by law.

In the event that any of your Personal Information is retained due to actual or anticipated court actions or other legal proceedings, it will be deleted after final conclusion of the event as appropriate.

Residents of EEA, Switzerland and UK

Legal Basis for Processing Personal Information

We process the Personal Information we collect to decide whether to enter into a contract of employment or engagement with you.

We may also process your Personal Information in our legitimate interests of reviewing applications, performing data analysis on our applicant pool, or to consider you for future roles. We have taken into account your rights and interests and concluded that our legitimate interests are not overridden by your privacy rights. If we require consent to process your Personal Information we will notify you of this beforehand. We may also process your Personal Information to comply with our legal obligations.

Rights and Choices for Residents of EEA, Switzerland and UK

Verkada respects your rights concerning your Personal Information. These rights, which may vary depending on your location, generally include the right to:

- **Request access** to your Personal Information (commonly known as a "data subject access request") to receive a copy of the Personal Information we hold about you
- **Request correction** of the Personal Information that we hold about you
- **Request erasure (or deletion)** of your Personal Information where there is no lawful basis for us to continue to process it or where you have exercised your right to object to processing (see below)
- **Object to processing** of your Personal Information where you believe we do not have a legitimate interest in processing your Personal Information, or you object to our processing of it for direct marketing purposes
- **Withdraw consent** where we rely on consent to process your Personal Information
- **Request the restriction (or suspension) of the processing** of your Personal Information
- **Request the transfer** of your Personal Information to another party
- **Request human review of decisions based solely on automated processing** that produce legal effects or similarly significant impacts

If you want to exercise your rights, please submit a request through our online form contact us at 833.280.5900.

Where we have relied on consent to process your Personal Information, you have the right to withdraw your consent at any time by submitting a request through our online form or contacting us at 833.280.5900. You also have the right to lodge a complaint with a supervisory authority (EU list found here; Swiss Federal Data Protection and Information Commissioner, UK Information Commissioner) if you are unhappy with how your Personal Information is being handled.

Data Transfers Outside the EEA, Switzerland, and the UK

Verkada has implemented safeguards to help ensure an adequate level of data protection where your Personal Information is transferred outside of the EEA, Switzerland, and UK, with our vendors and partners (e.g., implementing standard contractual clauses where appropriate).

Residents of California

The California Consumer Privacy Act ("CCPA") requires us to disclose information regarding the categories of personal information and sensitive personal information that we have collected about California consumers, the categories of sources from which the information was collected, the business or commercial purposes (as those terms are defined by applicable law) for which the information was collected, and the categories of parties to whom we disclose personal information. As used in this section, "personal information" shall have the meaning set forth in the CCPA.

Throughout this Candidate Privacy Policy, we describe the specific pieces of personal information and sensitive personal information we collect, the sources of that information, and how we share it. Under the CCPA, we also have to provide you with the "categories" of personal information and sensitive personal information we collect and disclose for "business or commercial purposes" (as those terms are defined by the CCPA).

In the twelve months leading up to the effective date of this Candidate Privacy Policy, we have collected and disclosed the following categories of personal information:

- identifiers, such as name, address, and email address
- professional/employment-related information, such as your employment history
- education information, such as your education history
- potentially legally protected information such as race or ethnicity
- disability information, such as health conditions
- audio or visual information, such as security footage, as well as other information relating to the security of our premises collected during in-person interviews or other parts of the recruitment process, and photographs or videos submitted
- background check information
- inference data about you, such as if we derive information about your role within a company
- other information that directly or indirectly identifies you

We do not require you to provide us with "sensitive personal information" during the recruitment process. However, if you voluntarily include such information in your resume or application materials, we will process it as part of your submission. You may voluntarily provide us with the following categories of sensitive personal information: (1) racial or ethnic origin; (2) disability status; (3) citizenship or immigration status; and (4) other sensitive information.

We process the categories of personal information identified above for the purposes described above in "How We Use Your Personal Information"

We collect the categories of personal information identified above from the sources identified in "How Your Personal Information Is Collected"

We describe our information disclosure practices in more detail in the section above on "How We Disclose Your Personal Information"

California residents have certain rights regarding their personal information. Subject to certain exceptions, if you are a California resident, you may request:

- access to your personal information, including the right to know the categories of personal information we have or will collect about you and the reason we will or have collected such information
- correction of the personal information that we have or will hold about you that is inaccurate
- deletion or removal of your personal information
- if applicable, certain information regarding the purpose for, and logic and outcome of, automated decisionmaking technology used to make a "significant decision" (as defined by California law)
- if applicable, opt out of the use of automated decisionmaking technology to make a "significant decision" or to appeal the decision to a human reviewer

You also have the right not to be discriminated against (as provided for in California law) for exercising your rights.

Exceptions to Your Rights: There are certain exceptions to these above rights. For instance, we may retain your personal information if it is reasonably necessary for us or our vendors to provide a service that you have requested, to comply with law, or to detect security incidents, protect against malicious, deceptive, fraudulent, or illegal

activity or prosecute those responsible for that activity.

Exercising Your Rights: To exercise one of the rights above, you may submit a request through our online form or contact us at 833.280.5900.

We will take reasonable steps to verify your identity before responding to a request, which may include requesting information so we can identify you within our records. You can also designate an authorized agent to make a request on your behalf. To do so, you must provide us with written authorization or a power of attorney, signed by you, for the agent to act on your behalf. You may still need to verify your identity directly with us.

California law places certain obligations on businesses that "sell" personal information to third parties or "share" personal information with third parties for "cross-context behavioral advertising" as those terms are defined under the CCPA. As noted above, we may use cookies and similar technologies from third-party analytics services that may result in the "sharing" of online identifiers and other identifiers (e.g., cookie data, IP addresses, device identifiers, general location information, usage information, email addresses) with analytics partners to help us analyze and understand use of the Site. In some cases, such practice may also constitute a "sale" of personal information under the CCPA. If you or your authorized agent would like to opt out of our "sharing" or "sale" of your information for such purposes, you may do so by clicking Your Privacy Choices on the footer of the Site. To opt-out of the "sharing" or "sale" of personal information that is not based on cookies or other tracking technologies, please contact emailmarketing@verkada.com.

The CCPA also allows you to limit the use or disclosure of your "sensitive personal information" (as defined in the CCPA) if your sensitive personal information is used for certain purposes. Please note that we do not use or disclose sensitive personal information in ways that create an opt-out right.

Residents of Australia

In this section, "personal information" will have the same meaning given to that term under the Privacy Act 1988 (Cth) ("Privacy Act").

The Privacy Act requires entities bound by the Australian Privacy Principles ("APPs") to have a privacy policy. Throughout this Candidate Privacy Policy, we describe the specific types of personal information and sensitive information we collect and hold, how we collect or hold your personal information, and the purposes for which your personal information is collected, held, used or disclosed.

We may use or disclose your personal information for the purpose for which it was collected as set out in this Candidate Privacy Policy. We may also use and disclose your personal information for a secondary purpose that is related to a purpose for which we collected it, where you would reasonably expect us to use or disclose your personal information for that secondary purpose.

Rights and Choices for Australian Residents

Subject to certain exceptions, you have rights under the Privacy Act and Spam Act 2003 (Cth) to:

- request access to your personal information
- ask us to update or correct any personal information that is inaccurate, incomplete or outdated
- opt out of receiving direct marketing communications from us

To exercise one of the rights above, you may submit a request through our online form or contact us at 833.280.5900.

You also have the right to not identify yourself or to use a pseudonym when

communicating with us, except if we are required or authorized by or under Australian law to respond to individuals who have identified themselves or it is impracticable for us to respond if you have not identified yourself.

Retention of Your Personal Information

Please see the "How Long We Keep Your Personal Information For" section above.

Data Transfers Outside Australia

We may disclose your personal information to third parties located outside Australia. The countries in which these third parties are likely to be located will depend on the circumstances. Some of these entities include:

- companies within our corporate group which are located in or conduct business in the U.S., Canada, selected European Union countries and Switzerland, the UK, Mexico, Taiwan, Japan, South Korea and Singapore
- our data hosting and other vendors located in the U.S., the EU and the UK

We will take reasonable steps to ensure that personal information that is disclosed to third parties located outside Australia will not be held, used or disclosed by the overseas recipients in a manner which is inconsistent with the APPs.

Complaints

In addition to the Contact process listed below for complaints, if you believe that we have not addressed your concerns, you may also lodge a complaint with the Office of the Australian Information Commissioner (which is the regulator responsible for privacy in Australia). All complaints must be made in writing to the Director of Compliance at GPO Box 5218, Sydney NSW 2001. Further information can be found on the OAIC website at www.oaic.gov.au or by calling 1300 363 992.

Residents of Canada

This section applies specifically to residents of Canada and supplements our Candidate Privacy Policy to help ensure compliance with the Personal Information Protection and Electronic Documents Act (PIPEDA) and related Canadian privacy laws.

For Canadian residents, where any conflicts exist between this section and the other sections of this Candidate Privacy Policy, this section takes precedence. All other provisions of this Candidate Privacy Policy continue to apply.

Rights and Choices for Canadian Residents

- Subject to exceptions set out under applicable privacy laws, individuals located in Canada have the right to access, update and correct inaccuracies in their Personal Information in our custody or control. You may also have the right to receive a copy of your information (including certain information in a structured, commonly used technological format), and have us share it with an authorized third party in certain circumstances.

Individuals in Canada also have the right to withdraw consent to the use and disclosure of their Personal Information, subject to legal and contractual restrictions and reasonable notice. Please note that even if you withdraw your consent, we may continue to retain your Personal Information in accordance with our legal obligations and retention practices.

To exercise these rights or if you have any questions or complaints regarding this privacy notice or our privacy practices, please see "How to Contact Us" below. We may collect certain Personal Information for the purpose of verifying your identity before responding

to your request.

For more information on your choices (including with respect to cookies), see "Cookies and Tracking Technologies" above.

Privacy Governance Policies and Practices

We are committed to protecting your Personal Information and have implemented policies and practices that govern our treatment of Personal Information, including but not limited to:

- policies that define the roles and responsibilities for our employees with respect to the treatment of Personal Information in our custody and control
- policies governing the retention and destruction of Personal Information that is designed to meet our legal obligations
- processes for responding to data subject requests and complaints concerning the handling of Personal Information in a timely and effective manner
- policies and procedures concerning the protection of Personal Information, including safeguards designed to protect Personal Information in our custody and control against loss or theft and unauthorized access, use or disclosure
- the designation of a Privacy Officer who is responsible for overseeing Verkada's compliance with applicable privacy legislation
- practices pertaining to privacy training and awareness for our personnel with access to Personal Information

Data Transfers Outside Canada

As set out under "Where Your Personal Information Is Stored and Processed" above, we and our vendors may access, store and otherwise process personal information outside of Canada (and specifically, the province of Québec), including the Australia, U.S., selected European Union countries and Switzerland, the UK, Mexico, Taiwan, Japan, South Korea and Singapore. We and our vendors may disclose your personal information if we are required or permitted by applicable law or legal process, which may include lawful access by foreign courts, law enforcement or other government authorities in the jurisdictions in which we or our vendors operate.

For information about our practices with respect to the use of vendors outside of Canada, please contact our Privacy Officer at policy@verkada.com.

Residents of Japan

This section applies specifically to residents of Japan and supplements this Candidate Privacy Policy to address compliance with the Act on the Protection of Personal Information of Japan (the "APPI"). In the event of any inconsistency between this section and other provisions of this Candidate Privacy Policy, this section will prevail. In this section, "Personal Information," "Personal Data," and "Retained Personal Data" have the meanings given to those terms under the APPI.

Data Transfers Outside Japan

In cases where we transfer your Personal Information to a third party located outside Japan, we will do so based on your consent or where one of the following applies:

(i) the recipient is located in a country or region designated by applicable laws and regulations as having a Personal Information protection regime equivalent to that of Japan (currently, the EU and the UK); or

(ii) the recipient has established and maintains a system necessary to continuously implement measures equivalent to those required of a Personal Information handling business operator in Japan. In the case of (ii), we will take necessary and appropriate safeguards in accordance with the APPI, such as contractual or organizational measures.

Rights and Choices for Japanese Residents

In accordance with the APPI, if you (or your authorized representative) request any of the following with respect to your Personal Information or Retained Personal Data held by us under the APPI, we will verify that the request was made by you (or your authorized representative) and respond in accordance with your rights under the APPI, including:

- notification of the purposes of use;
- disclosure of Retained Personal Data that identifies you;
- correction, addition, or deletion of Retained Personal Data that identifies you; or
- suspension of use, erasure, or cessation of provision to third parties.

To exercise any of the rights above, you may submit a request through our online form or contact us at 833.280.5900.

In accordance with the APPI, we may jointly use certain personal data with Verkada group companies and affiliates. The personal data subject to joint use is the Personal Information described in the "What Personal Information We Collect" section. The scope of joint users includes Verkada group companies and affiliates, and the purposes of this joint use are those described in the "How We Use Your Personal Information" section. Verkada Inc. is the party responsible for the management of this jointly used personal data.

Residents of Mexico

This section applies specifically to residents of Mexico and supplements our Candidate Privacy Policy. In the event of any conflicts between this section and the other sections of this Candidate Privacy Policy, this section takes precedence.

Sensitive Personal Data

We may collect and process certain Sensitive Personal Data only where strictly necessary and in accordance with applicable law as identified in the sections "What Personal Information We Collect" and "How We Use Sensitive Personal Information". Such data may include information related to race, ethnicity, employment or educational background, criminal record, health or disability status, where permitted. We will process such sensitive personal data only with your express and written consent, except where otherwise permitted or required by law.

Purposes and Legal Basis for Processing

Regarding the specific purposes for processing your information set forth in the section "How We Use Your Personal Information" described above, and in accordance with Mexican Law, we hereby inform you of the following classification:

Primary Purposes (necessary for the legal relationship)

- evaluating your skills, qualifications and suitability for the role
- conducting interviews and managing the recruitment process
- verifying information provided, including reference checks and work authorization
- performing background checks where required and legally permitted
- communicating with you regarding your application
- conducting internal audits and recruitment-related investigations
- evaluating your work authorization in the relevant geography
- review your application, resume, schedule interviews, and record and analyze the interview content using tools that leverage artificial intelligence, where permitted (these tools support human decision-making and do not

make hiring decisions)
- improve Verkada's recruitment processes and services
- complying with applicable legal or regulatory obligations

Secondary Purposes

- maintaining recruitment records
- retaining your profile information for consideration for future job opportunities (unless you object or request deletion of such information)
- performing workforce and applicant pool analytics, benchmarking, and reporting

You may refuse or object to the processing of your Personal Data for secondary purposes as described in the section "Rights and Choices for Mexico Residents" below. Exercising such rights will not impact your candidacy or the recruitment process for the specific role you are currently applying for.

Data Transfers Outside Mexico

Your Personal Information may be processed, stored, or accessed in countries other than Mexico, including in the US by Verkada affiliates, subsidiaries, vendors, and other authorized third parties which support our recruitment processes, such as:

- cloud hosting providers, applicant tracking systems, interview intelligence platforms, and background check providers; and

- affiliates, subsidiaries, parent companies, and entities under common control by Verkada which operate under the same internal privacy and security standards.

Verkada may also transfer your Personal Information to third parties that are not acting solely as our service providers, including where such transfers are necessary to:

- maintain or fulfill the legal relationship between you and Verkada;
- support business operations through affiliates or entities under common control that operate under consistent internal policies;
- comply with legal obligations or requests from competent authorities;
- establish, exercise, or defend legal rights;
- protect public interests or support the administration of justice; or
- an actual or potential buyer (and its agents or advisers) in connection with any actual or proposed purchase, merger or acquisition of any part of our business, or to other third parties in the voluntary or involuntary dissolution (bankruptcy) of our business, provided that we inform the third party it must use your Personal Information only for the purposes disclosed in this Privacy Policy.

Where required under applicable law, Verkada will obtain your consent prior to carrying out any transfer of your Personal Information.

To protect your Personal Information, Verkada requires its vendors to use technical and organizational safeguards that meet both legal standards and our own privacy commitments.

Rights and Choices for Mexico Residents

You may exercise your ARCO Rights—Access, Rectification, Cancellation, and Opposition—concerning your Personal Information. You also have the right to revoke your consent or limit how your Personal Information is used or disclosed.

To exercise your ARCO rights, y submit a request through our online form or contact us at 833.280.5900. Depending on the nature of your request, we may require additional information to verify your identity, confirm your legal authority (where applicable), and process your request. This information may include:

- Documentation verifying your identity or, where applicable, the authority of your

legal representative;
- Additional information regarding the data subject right(s) you wish to exercise; and
- Additional information necessary to help us locate your Personal Information.

We will respond to your completed request in accordance with Mexican law.

Residents of the Republic of Korea

This section applies specifically to residents of the Republic of Korea ("Korea") and supplements our Candidate Privacy Policy to address compliance with the Personal Information Protection Act (PIPA) and related Korean privacy laws.

For Korean residents, where any conflicts exist between this section and the other sections of this Candidate Privacy Policy, this section takes precedence. All other provisions of this Candidate Privacy Policy continue to apply.

Legal Basis for Processing Personal Information

We process your Personal Information as necessary for the steps required to enter into an employment contract with you, in accordance with Article 15(1)(4) of PIPA. We may also process your Personal Information to comply with legal obligations or based on your consent where required.

How We Share Your Personal Information

We share certain Personal Information with other Verkada group companies and trusted vendors who process it under binding contracts and only when a valid legal basis applies as described in "Legal Basis for Processing Personal Information". Verkada's vendors may include technology and recruiter systems, software providers, including AI-assisted tools for recruitment, recruitment and search agencies, testing or assessment institutions, survey tool providers, payment processors, travel management, our background checks providers, and benefits providers. Verkada group companies and Verkada's vendors may be located in Australia, Canada, selected European Union countries, the UK, the U.S., Japan, Mexico, Singapore, Switzerland and Taiwan. We entrust the processing of certain Personal Information to vendors who process your information solely on our behalf and under contractual obligations such as:

- Checkr (U.S.) – background verification and screening services
- Greenhouse (U.S.) - application management and recruitment workflow
- Zoom (U.S.) - video interview hosting/recording
- CodeSignal (U.S.) - skills assessment and evaluation services
- Google Drive (U.S.) - secure data storage and backup services
- Educational Institutions/Previous Employers - reference verification and qualification confirmation

We may also share Personal Information with Verkada group companies and affiliates for shared services, global operations, and internal business coordination. These third parties may process various types of Personal Information, including contact details, communications, service usage data, and other information as outlined in "What Personal Information We Collect."

We may also share Personal Information with the following third parties as necessary:

- Courts, tribunals, regulators, public authorities, and professional advisers (including immigration specialists, tax advisers, accountants, and lawyers) to comply with legal and regulatory obligations, respond to complaints, or participate in audits, court orders, warrants, subpoenas, administrative, regulatory, or judicial processes.
- Other third parties as necessary – for litigation, safety concerns, business transitions (such as mergers or acquisitions), or where you have provided consent

or disclosure is otherwise reasonable.

Data Transfers Outside of the Republic of Korea

In connection with the entrusted processing and third-party sharing described above, we transfer your information to recipients located in Australia, Canada, selected European Union countries, the UK, the U.S., Japan, Mexico, Singapore, South Korea, Switzerland and Taiwan.

Regarding international transfers of your Personal Information, you may contact us using the methods described in the "How to Contact Us" section below to request additional information about such transfers, including the safeguards we have in place to protect your data.

Where applicable, you may object to or request restrictions on the transfer of your Personal Information. Please note that, in certain cases, this may limit our ability to process your application or proceed with the recruitment process. You may also withdraw your consent to the extent that we rely on consent for a specific transfer, subject to applicable legal and contractual limitations.

Retention of Your Personal Information

Please see the "How Long We Keep Your Personal Information" section above.

Rights and Choices for Korean Residents

When we collect your Personal Information from sources other than yourself (such as business partners, social media platforms, or publicly available sources), you have the right to request information about the source of collection, the purpose of processing, and your right to suspend processing or withdraw consent. You also have the right, in connection with the use of AI assisted tools described in the "How We Use Your Personal Information" section, to request an explanation of the basis for any decisions involving such automated processing. In addition to the foregoing, you may exercise any other rights available to you as a data subject under PIPA.

If you require any further clarification regarding this Privacy Policy, or wish to exercise your rights regarding your personal data, please see "How to Contact Us" below.

Complaints

Our Domestic Representative of Korea Personal Information Protection Act is our Chief Privacy Officer (see "How to Contact Us" for more information). Korean residents can apply for dispute resolution or consultation to the following institutions for remedies for personal information infringement:

- Personal Information Infringement Report Center: (without area code) 118
- Personal Information Dispute Mediation Committee: (without area code) 1833-6972
- Supreme Prosecutors' Office Cybercrime Investigation Division: (without area code) 1301
- National Police Agency Cyber Investigation Bureau: (without area code) 182

Updates to this Candidate Privacy Policy

We may update this Candidate Privacy Policy from time to time in response to changing legal, technical or business developments. When we update our Candidate Privacy Policy, we will take appropriate measures to inform you, consistent with the significance of the changes we make and as required by applicable law. Please check back from time to time

to review the current Candidate Privacy Policy which is effective as of the revision date listed below.

How to Contact Us

Depending on where you are located and how you interact with Verkada, you may have certain legal rights over the Personal Information we hold about you, subject to local privacy laws. You can request to exercise any of your privacy rights above by submitting a request through our online form or contacting us at 833.280.5900.

If you require any further clarification regarding this Candidate Privacy Policy, please contact policy@verkada.com or our People Team using the contact details provided to you as part of your application. We will acknowledge your complaint in writing as soon as possible and will give you an estimated timeframe for when we will respond. Verkada's Chief Privacy Officer is Elizabeth Davies.

Verkada Inc. is a data controller of applicant and employee information in its role as parent company that makes strategic employment decisions.

If you are located in the EEA, UK, or Switzerland, Verkada Limited and VERKADA POLAND SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ may also be data controllers in their capacity as our European entities which help review and administer our recruitment process. In other cases, the local Verkada entity that would be your employer if your application is successful will also make decisions with regard to your application.

For office addresses of global Verkada company offices, please see the directory of our office locations.