Blanchard HR Privacy Policy

Policy Owner: Blanchard HR Privacy Policy
Applies To: All Blanchard Employees, Contractors, and applicants, and other workers
Effective Date: 3/01/2026
Review Cycle: Annually

Purpose

The purpose of this HR Privacy Policy is to describe how Blanchard collects, uses, discloses, stores, and protects personal information relating to employees, applicants, contractors, and other workers, and to ensure such processing complies with applicable privacy laws and data protection requirements.

Scope

This HR Privacy Policy applies to:

- Employees
- Job applicants
- Contractors and temporary workers
- Former employees (for the duration data is retained)

It covers personal information processed throughout the employment lifecycle, from recruitment to offboarding and post-employment record retention.

Policy Statement

Blanchard ("the Company," "we," "us," or "our") is committed to protecting the privacy and security of personal information relating to our employees, applicants, contractors, consultants, and other workers ("you" or "employees"). This HR Privacy Policy ("Policy") describes how we collect, use, disclose, store, and protect personal information processed in the context of recruitment and employment or work engagement.

This Policy is intended to comply with applicable privacy laws, including but not limited to the General Data Protection Regulation (GDPR), the UK GDPR, and the California Consumer Privacy Act (CCPA), as amended by the CPRA, where applicable. By proceeding with your application or employment engagement, you have been notified of and consent to the terms herein.

Categories of Personal Data We Collect

We collect information that identifies, describes, or is reasonably capable of being associated with you ("personal information") or your household. The following discusses the categories of personal information we collect, the sources from which we collect information.

We may collect and process the following categories of personal information:

- **Identifiers:** We may collect basic identity and contact information, like your real name, postal address, phone number, unique personal identifier, Internet Protocol address, email address, geolocation data, account name, unique

identifier of device, social security number, driver's license number, passport number, or other similar identifiers, that you provide us directly.

- **Personal Information Records**: We may collect other personal information that you submit to us, such as your name, signature, bank account number, credit card number, debit/card number, or other financial information.
- **Professional or Employment-Related Information**: We may collect details about your employment background, like position, work experience, and employment references.
- **Background Information**: Where relevant to your application and permitted under applicable law, we may collect background information relevant to employment, such as your educational background including degrees, transcripts, certifications, employment authorization status, and/or criminal background screenings.
- **Social and Professional Profiles**: We may collect links to your profiles on third party sites that may contain additional information relevant to your application.
- **IT and System Usage**: We may indirectly collect certain technical information from you about your visit to our website as an applicant, like your IP address and the date and time you submitted a form. As an employee of Blanchard, we may collect work device identifiers, login and access logs, and email/communication metadata (not content unless necessary for compliance, security, or investigations) while using Blanchard assets.
- **Application Documents**: We may collect documents or materials that you submit in connection with your application, like cover letters, resumes, coding exercises, written responses, and presentations.
- **Demographic Data**: We may ask for voluntary self-identification information related to demographic categories, in accordance with applicable law.
- **Recruitment Data**: We may store data about the recruitment/interview process, including resumes/CVs that you submit and information on the interview process including recruiter correspondence, schedules, and feedback, assessment results, and background check reports.
- **Offer Data**: We may store data about any offer that we make to you, including role, compensation, and benefits.
- **Performance and Development Data**: We may collect information generated internally and from you related to your performance, professional development, goals, feedback, training completion, and career progression.
- **Health and Accommodation Information**: Where permitted by applicable law, we may collect limited health-related information from you that is necessary to administer workplace accommodations, leaves of absence, or benefits. Such information is handled confidentially and only used for lawful purposes.
- **Compliance and Investigations Data**: We may directly or indirectly collect and process information as necessary to comply with legal obligations, internal policies, or to investigate potential violations, including information related to complaints, investigations, audits, or legal proceedings.
- **Payroll and Benefit Data**: We may collect and store information related to your compensation and benefits, including bank details for payroll, tax withholding information, benefit and health plan enrollment elections, dependent and beneficiary information, and emergency contact details. Where applicable, this may include information necessary to administer health, wellness, or insurance benefits in accordance with law.
- **Sensitive Personal Information**: Where required by law, we may collect information that you provide, such as your social security, driver's license, passport number, other government-issued identification numbers, or employment authorization documents to verify your identity and eligibility to work. This information is collected solely for compliance with applicable employment and immigration laws.

Special Categories of Personal Data and Protected Classification Characteristics

Blanchard does not require you to submit sensitive personal information or special category personal data such as data relating to religion, health, sexual orientation, trade union affiliation, race, ethnicity, physical or mental disability, veteran or military status, or political opinion in connection with your application.

Based on local law, we may ask for information like race, ethnicity, or gender so that we can ensure that we are meeting local reporting requirements and to provide equal employment opportunities.

If you choose to provide us with sensitive or special category personal data, you are expressly consenting for us to handle such data in accordance with this Policy.

Data from Third Parties

We may obtain information about you from public sources or third parties. For example, we may obtain information about you from individuals who have referred you to us and recruiting service providers who may collect your personal data from publicly available sources. You may also choose to give us access to personal data stored by third parties, like your profile on a job-related social media site. By providing us with this access, you agree that we may collect and use this information in accordance with this Policy. We may also conduct background screenings through a third-party service provider and verify application information, like your education, employment, and/or criminal history, as allowed by applicable law.

Purposes for Processing Personal Data

We process personal data for legitimate business purposes, including:

- **Recruitment & Hiring**: We may process personal data in order to communicate with you and inform you of the status of your application and future opportunities. Communication may include recruitment, evaluation, and selection of job candidates (temporary or permanent) for the job applied for and subsequent opportunities. Communication may also include application evaluation, like verification of employment reference(s) that you provide, background checks, and related assessments.
- **Employment Administration**: We may store data for processing general employment administration and management information such as payroll, expense reimbursement, benefits administration, timekeeping and attendance, scheduling and resource planning.
- **Legal & Compliance Obligations**: To remain compliant with corporate governance and legal requirements, we may process personal data for tax reporting, employment law recordkeeping, occupational health and safety, and responding to legal claims or regulatory requests.
- **Security & IT Administration**: We may process personal data in order to provide you access to systems and tools, monitor for cybersecurity threats, and protect company assets and confidential information.
- **Performance & Development**: As an employee of Blanchard, we may process personal data as it relates to performance reviews, coaching, learning, and development programs, and promotions and career progression.
- **Workplace Management**: We may process personal data as it relates to office access and security, and travel and expense management.

We only process personal information for legitimate business purposes.

Legal Bases for Processing (GDPR / UK GDPR)

Where GDPR or UK GDPR applies, we process personal data under one or more of the following lawful bases:

- **Performance of a contract** (employment agreement)
- **Legal obligations** (e.g., tax, employment laws)
- **Legitimate interests** (e.g., security, workforce management) – balanced against your rights
- **Consent**, only where required and freely given (e.g., optional DEI disclosures)
- **Vital interests** (e.g., emergency situations)

For **special-category data**, processing of personal data subject to the GDPR or UK GDPR occurs only when legally permitted, including:

- Employment, social security, and social protection law obligations
- Explicit consent
- Public health or workplace safety requirements

You are required to provide the personal data requested that is necessary for Blanchard to fulfill its contractual obligations in your employee agreement. Failure to provide your data or information will affect Blanchard's ability to consider your candidacy or provide employment. Blanchard limits your personal data collected to the information necessary to fulfill its obligations and the legal bases.

How We Disclose Personal Information

Your personal data may be shared internally such as People & Culture department, managers and supervisors, payroll and finance departments, and IT and security teams as described in Section 3 ("Purpose for Processing Personal Data").We also disclose or make available your personal data only with those who need it in order to perform their tasks and duties for the purposes described above. We may disclose your personal data to the following types of third parties:

- **Third-Party Service Providers and Contractors:** We may disclose your personal data with our third-party service providers and contractors who provide services like recruiting, background screening, and applicant management, payroll processors, benefit and insurance providers, HR information systems (HRIS) vendors, background check agencies, recognition and wellness platforms, employee administration management, and training and coaching platforms.
- **Legal and Security:** We may disclose your data with parties as needed for security or legal compliance reasons such as tax authorities, courts or government agencies, law enforcement (when legally required).
- **Business Transfers:** If Blanchard undergoes a business transaction like a merger, acquisition, corporate divestiture, or dissolution (including bankruptcy), or a sale of all or some of our assets, we may disclose, make available, or transfer all of your data to the successor organization during such transition or in contemplation of a transition (including during due diligence). We **never** sell employee personal information for any purpose, and under the CCPA, we do not sell or share employee personal information for targeted or cross-context behavioral advertising.

These third parties are legally required and contractually obligated to handle any disclosed personal data solely as we direct and to treat your personal data in a confidential manner.

International Transfers

For EU and UK employees, contractors, and applicants, as our recruiting operations are based in the United States, we transfer your personal data to the United States for processing consistent with the purposes stated in Section 3. Personal data will be processed outside of the UK, Switzerland, and the European Economic Area ("EEA") by Blanchard or its service providers to provide support services as described above in the section entitled "Who We Share Your Data With". We have entered into data processing agreements with our external service providers or data processors abroad to restrict and regulate their processing of your data in accordance with this Policy. We use Standard Contractual Clauses (SCCs) adopted by the European Commission to facilitate international transfers of personal data. You have the right to obtain a free copy of the SCCs. You may use the information in the section below entitled "Updates and Contact Info" to submit requests related to data protection.

You have the right to lodge a complaint with your EU data supervisory authority. For UK residents, you may submit a complaint with the UK Information Commissioner's Office (ICO). Please see the ICO's website for more information: www.ico.org.uk.

By submitting your data to us, you are agreeing to this transfer, storage, and processing by Blanchard and its service providers.

Data Retention

We retain personal data only as long as necessary for:

- Purposes described in Section 3
- Employment and HR operations
- Legal and regulatory obligations, including record keeping
- Defense against legal claims

Retention periods vary by jurisdiction and data category; Blanchard maintains an internal retention schedule.

Your Rights

Under GDPR (EU/UK), you have the right to:

- **Access your personal data**. You have the right to ask us for copies of your personal data.
- **Request correction or updating**. You have the right to ask us to rectify personal data you think is inaccurate. You also have the right to ask us to complete information you think is incomplete.
- **Request deletion** ("right to be forgotten"). You have the right to ask us to erase your personal data in certain circumstances.
- **Object to or restrict processing**. You have the right to ask us to restrict the processing of your personal data in certain circumstances.
- **Request data portability**. You have the right to ask that we transfer the personal information you gave us to another organization, or to you, in certain circumstances.
- **Withdraw consent** at any time if the processing of your personal data is based on your consent.

Under CCPA (California), you have the right to:

- **Request to know and access** what categories of personal information we collect and use.
- **Request deletion** of your information collected subject to certain exceptions.
- **Request correction** of any inaccurate personal information we may hold about you.
- **Not be discriminated against** for exercising your privacy rights.

California residents maintain the right to opt-out of "selling" or "sharing" of personal information used for cross-context behavioral advertising as defined by the CCPA; however, Blanchard **does not sell or share** any employee data for targeted or cross-context behavioral advertising purposes.

To exercise your applicable rights, requests can be submitted through People and Culture or via: privacyofficer@blanchard.com.

Security Measures

We use appropriate technical and organizational security measures, based on the type and sensitivity of data being stored, to protect against unauthorized access, alteration, disclosure, or destruction of your personal data that we collect and store.

We use administrative, technical, and physical safeguards to protect personal information as appropriate.

However, as no system can be 100% secured, we cannot guarantee against unauthorized access by third parties. We continuously evaluate and improve our security posture.

Automated Decision-Making

Blanchard does not use automated decision-making, including profiling, or automated decision-making technology that produces decisions or outputs with legal or significant effects on employees without human involvement, as defined by GDPR, UK GDPR, or the CCPA.

If this ever changes, we will provide required disclosures.

Changes to This Policy

We may update this Policy periodically. Any material changes will be communicated through internal channels.

Contact Information

If you have questions or want to exercise your privacy rights, contact:

Blanchard –Compliance
Email: PrivacyOfficer@blanchard.com
Address: *125 State Place, Escondido, CA. 92029*

Related Documents

Links to:

- General Privacy Policy and Notice at Collection

Review & Maintenance

This policy will be reviewed annually.

Review

This policy will be reviewed annually and updated as necessary to reflect changes in laws, expectations, and our business practices.

Revision History

Version	Date	Author (s)	Approved By	Description of Change
Version 1.0	2/24/2026	Cathy Paiva	Nikki Camacho	Creation and proofing