Corsair Human Resources Privacy Notice for California Residents

Corsair Memory, Inc. ("Corsair") is providing this Corsair Human Resources Privacy Notice ("**HR Privacy Notice**") to give its California employees, job applicants, contractors, and other individuals (collectively "**Personnel**") whose Personal Information is collected for purposes set out hereinafter (such as dependents). This HR Privacy Notice provides information regarding how we collect and use your Personal Information for the above mentioned purposes. In this **HR Privacy** Notice, "**Personal Information**" has the meaning given to the term in the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 (CPRA) (collectively, CCPA*).*

This HR Privacy Notice applies **only to Personal Information of California Residents** used in the context of human resources, employment, and other internal business functions relating to our Personnel and their family members or beneficiaries, including internal computer systems, networks, and online services. Corsair's public-facing Privacy Policy ("**Privacy Policy**") describes how we collect, use and protect the Personal Information of consumers and users of Corsair's products and services.

If you are a current Corsair employee, you can send an email to the Human Resources ("HR") Department at hr@corsair.com if you have any questions with respect to this HR Privacy Notice. You may also contact your local HR manager for assistance. If you are a contractor, an applicant, a former employee or a family member, please contact us at the address or email listed below for assistance. Please note, if you wish to access or update your information, you may be able to do so directly through online services or the Corsair portals.

PURPOSES FOR COLLECTING, USING, AND DISCLOSING PERSONAL INFORMATION

Corsair collects, uses, discloses, and retains Personal Information processed under this HR Privacy Notice about its prospective, current, and former Personnel, for recruitment, employment, employee benefits, financial, and IT/technical support services, and internal software, networks, devices and legal compliance. The categories of Personal Information we process, along with representative data elements, and purposes are listed below:

A. Personal Information pertaining to *prospective* employees or contractors may be processed for the following purposes:
   i.   **Employment/Benefits**
       *   Evaluating prospective employment/engagement.
       *   Recruiting and staffing assessment, including evaluating skills and job placement.
       *   Conducting reference checks.
       *   Tracking application status and application follow ups, activities.
       *   Making hiring decisions, including negotiating compensation, benefits, relocation packages, etc.
   ii. **Immigration Management**
       *   Determining an individual's eligibility to work.
       *   Processing work permits or visas.
   iii. **IT Services**
       *   Analyzing job post activity and recruitment website traffic statistics and aggregate user behavior.
   iv. **Background Checks**

- Conducting background checks, vetting and verification, consumer credit reporting, and conducting related assessments (where permitted by law).

    v. **Legal**
    - Reporting to EEOC and other federal/state government-related reporting.
    - Protecting against liability, complying with lawful governmental investigations or requests, and enforcing our policies and agreements.

B. <u>Personal Information pertaining to *current* employees and contractors may be processed for the following purposes</u>:

    i. **Employment/Benefits**
    - Evaluating, creating, and maintaining the employment relationship.
    - Administering payroll and compensation.
    - Administering insurance and benefits programs e.g. dental, FSA, HSA, etc.
    - Hiring and job placement.
    - Conducting reference checks.
    - Time and attendance tracking, scheduling, managing absences, administering other workplace tasks, and facilitating relationships within Corsair.
    - Developing talent and performance, managing skills, training, conducting performance reviews (including customer surveys), conducting engagement surveys, and administering recognition and reward programs.
    - Conducting HR support services, such as responding to inquiries, providing information and assistance, and resolving disputes.
    - Conducting salary market surveys.
    - Recordkeeping and verifying employment/income.

    ii. **Financial Administration**
    - Handling reimbursements for expenses and expenditures.
    - Invoicing.
    - Administering ESOP/401k/investment plans.
    - Conducting salary surveys.

    iii. **Immigration Management**
    - Evaluating and maintaining visa eligibility.
    - Verifying right to work/eligibility.

    iv. **IT Services**
    - Managing our computers and other IT assets.
    - Supporting our systems and promoting security.
    - Providing email and other communications and software services.

    v. **Internal Programs**
    - Conducting diversity, equity, and inclusion initiatives and programs.
    - Conducting health and wellness programs.

    vi. **Health and Safety**
    - Conducting occupational health and safety programs (including required reporting, disaster and pandemic planning, vaccination status tracking, and managing incidents);
    - Making and assessing disability accommodations.
    - Conducting anti-harassment training.

    vii. **Risk Management and Loss Prevention**
    - CCTV and premises monitoring, such as in warehouses, or adjacent to Corsair premises, and managing/authenticating on-site access.

- Recording calls for training purposes.
- Monitoring IT systems for security and support purposes.

viii. Background Checks
- Conducting background checks, vetting and verifying, consumer credit reporting, and conducting related assessments (where permitted by law).

ix. Legal
- ACA and IRS reporting.
- EEOC and federal/state government reporting.
- Protecting against liability, complying with lawful governmental investigation or request, enforcing our policies and agreements.

C. <u>Personal Information pertaining to *former* employees and contractors may be collected, used and shared for</u>:

i. Employment/Benefits
- Evaluating, creating, and maintaining the employment relationship in the event of re-employment.
- Administering insurance and benefits programs e.g. dental, FSA, HSA, etc.
- Archiving and recordkeeping.
- Verifying employment and income.

ii. Financial Administration
- Administering ESOP/401k/investment plans.

iii. Legal
- ACA and IRS reporting.
- Protecting against liability, complying with lawful governmental investigation or request, enforcing our policies and agreements.

D. <u>Personal Information pertaining to individuals whose information is provided to Corsair in the course of HR management (such as information pertaining to employees' family members, beneficiaries, dependents, emergency contacts, *etc.*) may be collected, used and shared for</u>:

i. Employment/Benefits
- Administering insurance and benefits programs e.g. dental, FSA, HSA, etc. ;
- Complying with child support orders or garnishments.
- Maintaining internal directories, emergency contact lists and similar records.

ii. Legal
- Protecting against liability, complying with lawful governmental investigation or request, enforcing our policies and agreements.

E. <u>All Personal Information may be processed for our business purposes, which includes the following purposes ("**Business Purposes**")</u>:
   i. Managing identity and credentials, including verifying and authenticating identity, issuing ID cards and badges, administering systems, and managing access credentials.
   ii. Administering security, loss prevention, information security and cybersecurity.
   iii. Complying with laws and regulations, including without limitation all uses and disclosures of Personal Information that are required by law or for compliance with legally mandated policies and procedures, such as anti-money laundering programs, security and incident response programs, intellectual property protection programs, and corporate ethics and compliance hotlines, and other processing in connection with establishing of and defending against legal claims.
   iv. Auditing, analyzing, and consolidated reporting.

v.   Enforcing our contracts and protecting Corsair, our workers, our clients and their employees, and the public against injury, theft, legal liability, fraud or abuse, to people or property.
vi.   As needed for de-identifying data or creating aggregated datasets, such as for consolidating reporting, research, or analytics.
vii.   Making back-up copies for business continuity and disaster recovery purposes, and other IT support, debugging, security, and operations.
viii.   Analyzing and improving technical and organizational services and operations.
ix.   As needed for facilitating corporate governance, including mergers, acquisitions and divestitures.

CATEGORIES OF PERSONAL INFORMATION

This chart describes the categories of Personal Information that Corsair may collect in connection with its employment and contractual work relationships. Note, all Personal Information may be used and disclosed in connection with our Business Purposes.

Category of PI and Representative Data Elements	Common Purposes for Collecting and Sharing the PI
Contact Data Examples: • Honorifics and titles, preferred form of address. • Mailing address. • Email address. • Telephone number. • Mobile number. • Social media or communications platform usernames or handles.	• Employment/Benefits. • Financial Administration. • ImmigrationManagement. • IT Services. • Internal Programs. • Health and Safety. • Risk Management and Loss Prevention. • Background Checks • Legal.
Identity Data Examples: • Full name, nicknames or previous names (such as maiden names), • Date of birth. • Language. • Company ID number. • Company account identifiers and passwords. • Benefits program identifiers. • System identifiers (e.g., usernames or online credentials).	• Employment/Benefits. • Financial Administration. • ImmigrationManagement. • IT Services. • Internal Programs. • Health and Safety. • Risk Management and Loss Prevention. • Background Checks. • Legal.
Government ID Data Examples: • Social security number. • Driver's license number. • Passport number.	• Employment/Benefits. • Financial Administration. • Immigration Management. • Background Checks. • Legal.

Category of PI and Representative Data Elements	Common Purposes for Collecting and Sharing the PI
• Other government-issued identifiers as may be needed for risk management or compliance (*e.g., if you are a licensed professional, we will collect your license number*).	
Biographical Data Examples: • Resume or CV. • Data from LinkedIn profiles and similar platforms. • Education and degree information. • Professional licenses, certifications, memberships, and affiliations. • Personal and professional skills and talents summaries (e.g., languages spoken, CPR certification status, community service participation), interests, and hobbies. • Professional goals and interests.	• Employment/Benefits. • Immigration Management. • Internal Programs. • Risk Management and Loss Prevention. • Background Checks.
Transaction and Interaction Data Examples: • Dates of Employment. • Re-employment eligibility. • Position, title, department, reporting information. • Work history information. • Time and attendance records. • Leave and absence records. • Salary/Payroll records. • Benefit plan records. • Travel and expense records. • Training plan records. • Performance records and reviews. • Disciplinary records.	• Employment/Benefits. • Financial Administration. • Immigration Management. • Internal Programs. • Health and Safety. • Risk Management and Loss Prevention.
Financial Data Examples: • Bank account number and details. • Company-issued payment card information, including transaction records. • Personal payment card information, if provided for reimbursement • Credit history, if a credit check is obtained (only done in limited circumstances).	• Employment/Benefits. • Financial Administration. • Risk Management and Loss Prevention. • Background Checks.
Health Data	• Employment/Benefits. • Internal Programs.

Category of PI and Representative Data Elements	Common Purposes for Collecting and Sharing the PI
Examples: • Medical information for job placement, including drug testing and fitness to work examinations, accommodation of disabilities. • Medical information for leave and absence management, emergency preparedness programs. • Dietary restrictions or information. • Wellness program data. • Information pertaining to enrollment and utilization of health and disability insurance programs.	• Health and Safety. • Legal.
Device/Network Data Examples: • Device information from devices that connect to our networks. • System logs, including access logs and records of access attempts. • Records from access control devices, such as badge readers. • Information regarding use of IT systems and Internet access, including metadata and other technically-generated data. • Records from technology monitoring programs, including suspicious activity alerts. • Data relating to use of communications systems and content of those communications.	• Employment/Benefits. • Financial Administration. • Immigration Management. • IT Services. • Internal Programs. • Risk Management and Loss Prevention.
Audio/Visual Data Examples: • Photograph. • Video images, videoconference records. • CCTV recordings. • Call center recordings and call monitoring records. • Voicemails.	• Employment/Benefits. • IT Services. • Risk management and loss prevention.
Inference Data Examples: • Performance reviews. • Results of tests related to interests and aptitudes.	• Employment/Benefits. • Internal Programs. • Health and Safety. • Risk Management and Loss Prevention. • Background Checks. • Legal.
Compliance and Demographic Data Examples: • Diversity information.	• Employment/Benefits. • Internal Programs. • Health and Safety. • Risk Management and Loss Prevention.

Category of PI and Representative Data Elements	Common Purposes for Collecting and Sharing the PI
• Employment eligibility verification records, background screening records, and other records maintained to demonstrate compliance with applicable laws, such as payroll tax laws, ADA, FMLA, and ERISA. • Occupational safety records and worker's compensation program records. • Records relating to internal investigations, including compliance hotline reports. • Records of privacy and security incidents involving HR records, including any security breach notifications.	• Legal.
Protected Category Data Examples: Characteristics of protected classifications under California or federal law, e.g. race, national origin, religion, gender, or sexual orientation. **Sensitive Personal Information** Examples: Personal information that reveals: (A) social security, driver's license, state identification card, or passport number; (B) account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account; (C) precise geolocation; (D) racial or ethnic origin, religious or philosophical beliefs, or union membership; (F) genetic data; (G) biometric information; (H) health information; or (I) personal information regarding sex life or sexual orientation.	• Employment/Benefits. • Financial Administration. • Immigration Management. • Health and Safety. • Risk Management and Loss Prevention. • Background Checks. • Legal.

CATEGORIES OF SOURCES OF PERSONAL INFORMATION

We collect Personal Information from various sources, which vary depending on the context in which we process that Personal Information.

- **Data you provide us** – We will receive your Personal Information when you provide it to us, when you apply for a job, complete forms, or otherwise direct information to us.
- **Data we collect automatically** – We may also collect information about or generated by any device you use to access IT services, applications, and networks.
- **Data we receive from service providers** – We receive information from service providers performing services on our behalf.
- **Data we create or infer** – We (or third parties operating on our behalf) create and infer Personal Information such as Inference Data based on our observations or analysis of other Personal Information processed under this HR Privacy Notice, and we may correlate this information with other information we process about you. We may combine Personal Information about you that we receive from you and from third parties.

DISCLOSURE OF PERSONAL DATA

We generally process Personal Information internally; however, it may be shared or processed externally by third party service providers, when required by law or necessary to complete a transaction, or in other circumstances described below.

CATEGORIES OF INTERNAL RECIPIENTS

The Personal Information identified below collected from our Personnel may be disclosed to the following categories of recipients in relevant contexts.

- **Personnel of HR Departments** – All Personal Information relating to human resources and recruitment.

- **Personnel of Finance Departments** – Personal Information to the extent related to company and employee transactions.

- **Direct Supervisors –** Elements of Personal Information to the extent permitted in jurisdiction, to the extent necessary to evaluate, establish, and maintain the employment relationship, conduct reviews, handle compliance obligations, and similar matters.

- **Department Managers Searching for new Employees** – Personal Information of job candidates contained in job applications to the extent allowed by relevant laws and departmental needs.

- **Senior Supervisors –** Elements of Personal Information to the extent permitted in jurisdiction, to the extent necessary to evaluate, establish, and maintain the employment relationship, conduct reviews, handle compliance obligations, and similar matters.

- **IT Administrators** of Corsair and/or third parties who support the management and administration of HR processes may receive Personal Information as necessary for providing relevant IT-related support services (conducting IT security measures and IT support services).

- **Peers and Colleagues –** Elements of Personal Information, to the extent permitted in jurisdiction, in connection with company address books, intracompany and interpersonal communications, and other contexts relevant to the day-to-day operation of company business.

CATEGORIES OF EXTERNAL RECIPIENTS

Corsair may provide Personal Information to external third parties as described below. The specific Personal Information disclosed may vary depending on context but will be limited to disclosures permitted by law. We generally provide Personal Information to:

- Our subsidiaries, affiliates, and parent company.

- Service providers, vendors, and similar data processors that process Personal Information on Corsair's behalf (e.g., analytics companies, financial analysis/budgeting, trainings, benefits administration, payroll administration, etc.).

- Prospective sellers or buyers of such business or assets in the event Corsair sells or buys any business or assets or engages in a merger or similar transaction.

- Future Corsair affiliated entities, if Corsair or substantially all of its assets are acquired by a third party, in which case Personal Information held by it about its employees will be one of the transferred assets.

- Government agencies or departments, employee unions, or similar parties in connection with employment-related matters.

- Any public authority in relation to national security or law enforcement requests, if Corsair is required to disclose Personal Information in response to lawful requests by public authority.
- Any other appropriate third party, if Corsair is under a duty to disclose or share your Personal Information to comply with any legal obligation or to protect the rights, property, or safety of Corsair, our employees, customers, or others.

SECURITY

Corsair requires that Personal Information be protected using technical, administrative, and physical safeguards, as described in our security policies. Corsair staff must follow the security procedures set out in applicable security policies at all times.

RETENTION AND DISPOSAL

Corsair keeps Personal Information only for the amount of time it is needed to fulfill the legitimate purpose for which it was collected or to satisfy a legal requirement. Corsair staff must follow applicable records retention schedules and policies and destroy any media containing Personal Information in accordance with applicable company policies.

CONTACT

Corsair Memory, Inc.

hr@corsair.com
Last Updated & Effective: May 25, 2023