FCA US LLC ("FCA," "we" or "us") Employee Privacy Notice

Effective Date: January 1, 2023

INTRODUCTION

This FCA Employee Privacy Notice (the "**Employee Notice**" or "**Notice**") Employee Notice is designed to supplement other FCA policies and corporate process guidelines (collectively "**FCA Policies**") and to notify Employees about our information practices. In this Employee Notice, we describe our collection and use of personal information about current and former full-time, part-time and temporary Employees and staff, as well as FCA officers, directors, and owners (each an "**Employee**"). For California residents, this notice also is intended to satisfy our applicable notice requirements under the California Consumer Privacy Act and the regulations issued thereto (collectively, the "CCPA"). We may provide Employees additional notices about our data collection practices that are covered by other laws (e.g., if we conduct a background check or collect health information).

SCOPE OF THIS NOTICE

This Employee Notice applies to personal information that we collect from and about our Employees, in the context of your employment relationship with FCA including personal information that we process to manage our employment relationships, administer benefits to Employees, grant and control access to our systems and assets (including the Employee Portal), and process Employee onboarding and terminations, as well as personal information we receive related to Employee beneficiaries, dependents and emergency contacts.

What isn't covered by this notice.

This Employee Notice does not address or apply to our collection of personal information that is not subject to the CCPA, such as protected health information (or "PHI"), consumer credit reports and background checks, publicly available data lawfully made available from state or federal government records, or other information that is exempt under the CCPA. This Employee Notice also does not apply to the personal information we collect from contractors or job applicants (which are subject to separate privacy notices), or from customers or end users of our products and services, including Employees, in the context of their personal use of FCA products and services, which is subject to the FCA US Privacy Policy.

Are our practices the same for all Employees?

The categories of personal information we collect, and our use of personal information may vary depending upon the circumstances, such as an Employee's role and responsibilities with FCA. In addition, if you visit one of our offices or locations, we may collect information as part of our onsite security. The information in this Employee Notice is intended to provide an overall description of our collection and use of personal information about Employees.

CATEGORIES OF PERSONAL INFORMATION COLLECTED

Generally, we may collect (and have in the prior 12 months collected) the following categories of personal information about Employees and disclose it to certain categories of third parties as for a business or commercial purpose as described below, to the extent permitted under applicable law. In some cases (such as where required by law), we may ask for consent or give you certain choices prior to collecting or using certain personal information.

Category	Third Parties Disclosures for Business or Commercial Purposes
Name, contact information and other identifiers: such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, Social Security Number, driver's license number, passport number, or other similar identifiers.	• service providers • advisors and agents • benefit providers • affiliates and subsidiaries • regulators, government entities and law enforcement • internet service providers, operating systems, and platforms • others as required by law
Paper and electronic records: paper and electronic records that may contain name, signature, Social Security Number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information, where relevant (e.g., as part of an Employee fleet program benefit that may be made available to certain Employees).	• service providers • advisors and agents • benefits providers • affiliates and subsidiaries • regulators, government entities and law enforcement • internet service providers, operating systems, and platforms • others as required by law
Characteristics of protected classifications: such as race/ethnicity, gender, sex, age, religion, veteran status, national origin, disability, citizenship status, and genetic information, and other characteristics of protected classifications under California or federal law. (Note: generally, this information is collected on a voluntary basis, after an offer of employment has been extended, and is used in support of our equal opportunity and diversity and inclusion efforts or where otherwise required by law.)	• service providers • advisors and agents • benefit providers • affiliates and subsidiaries • regulators, government entities and law enforcement • others as required by law
Biometric information: physiological, biological or behavioral characteristics that can be used alone or in combination with each other to establish individual identity, including DNA, imagery of the iris, retina, fingerprint, faceprint, hand, palm, vein patterns, and voice recordings, keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.	• service providers • advisors and agents • others as required by law
Internet or other electronic network activity information: including browsing history, search history, and information regarding a resident's interaction with an internet website, application, or advertisement, as well as physical and network access logs and other network activity information related to your use of any FCA device, network or other information resource, if applicable.	• service providers • advisors and agents • beneift providers • affiliates and subsidiaries • regulators, government entities and law enforcement

	• internet service providers, operating systems, and platforms • others as required by law
Geolocation Data: precise geographic location information about a particular individual or device.	• service providers • advisors and agents • affiliates and subsidiaries • internet service providers, operating systems, and platforms • others as required by law
Audio, video and other electronic data: audio, electronic, visual, thermal, or similar information, such as, CCTV footage, photographs, and call recordings and other audio recording (e.g., recorded meetings and webinars).	• service providers • advisors and agents • benefit providers • affiliates and subsidiaries • regulators, government entities and law enforcement • others as required by law
Employment history: professional or employment-related information.	• service providers • advisors and agents • benefit providers • affiliates and subsidiaries • others as required by law
Education information: information about education history or background that is not publicly available personally identifiable information as defined in the federal Family Educational Rights and Privacy Act (20 U.S.C. section 1232g, 34 C.F.R. Part 99).	• service providers • advisors and agents • affiliates and subsidiaries • others as required by law
Inferences drawn from personal information collected: inferences used to create a profile about an individual reflecting her or his preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.	• service providers • advisors and agents • benefit providers • affiliates and subsidiaries • others as required by law
Sensitive personal information: such as Social Security Number, driver's license number, passport number, race or national origin (e.g., on a voluntary basis to support of our equal opportunity and diversity and inclusion efforts and reporting obligations, or where otherwise required by law, or union membership), biometrics (e.g., for timekeeping and access controls), and health information (e.g., as necessary to provide reasonable accommodations).	• service providers • advisors and agents • benefit providers • affiliates and subsidiaries • others as required by law

We do not sell or share (as defined by the CCPA) Employee's personal information, including sensitive personal information, with third parties, including those we know who are under the age of 16.

SOURCES OF PERSONAL INFORMATION

In general, we may collect Employee personal information identified in the table above from the following categories of sources:

- Directly from you
- Recruiters and recruiting platforms
- Referrals and references
- Former Employees
- Other Employee
- Publicly available information and data brokers
- Service providers, representatives and agents
- Affiliates and subsidiaries

PURPOSES FOR COLLECTING AND USING PERSONAL INFORMATION: Generally, we may use the above categories of personal information for the following business or commercial purposes:

- Compensation, benefits, and Employee programs: relating to our administration of compensation and benefits, including:
    - Administering Employee payroll, salary, and compensation
    - Travel and expense reimbursement
    - Administering Employee pensions, IRAs and 401K, health insurance, medical plans, and other Employee benefits administration (which may include the collection of personal information about others such as beneficiaries, where necessary to administer such benefits)
    - Administering other Employee rewards and programs, such Employee fleet program benefits and Employee purchase programs, that may be made available to certain Employees
    - Reviewing, assessing, and administering Employee salary and compensation increases and bonuses
    - Calculating deductions, issuing tax return-related documents and forms to Employees
    - Reviewing timecards and reported time worked
    - Monitoring and managing PTO, holiday, FMLA, and other leaves of absences
- Management of employment relationships: to manage our relationship with Employees, including for:
    - Hiring, terminations, relocation, transfers, promotions, and disciplinary actions
    - Reviewing performance
    - Conducting Employee performance reviews, compensation and bonus reviews, and headcount and salary reviews
    - Providing training and career development
    - Tracking attendance, time entries and working hours
    - Administering and monitoring compliance with our policies and procedures
    - Maintaining records of emergency contact information for use in the event of an emergency
    - Administering or performing employment contracts where applicable
    - Conducting pre-employment and employment screening
    - For professional development and training purposes and to ensure you have and maintain the correct qualifications and skills to perform your role and identify any future training needs
    - Verification and management of applicable Employee credentials, licensing, memberships, and other qualifications

    - Facilitating Employee communication and collaboration, such as through the corporate directory, Employee bios and other similar
    - In support of our equal opportunity employment policy and diversity and inclusion program, including monitoring and reporting on equal opportunity
- Business operations and client services: relating to the organization and operation of our business and our performance of services to clients, including related to:
    - Operating our business by developing, producing, marketing, selling, and providing goods and services
    - Conducting Employee surveys
    - Providing after-sales services to clients
    - Auditing and assessing performance of business operations, including client services and associated activities
    - Training and quality control
    - Satisfying client reporting and auditing obligations
    - Facilitating business development opportunities, as relevant
    - Facilitating communications in furtherance of the foregoing
- Security and monitoring: to monitor and secure our resources, network, premises, and assets, including:
    - Monitoring for, preventing, investigating, and responding to suspected or alleged misconduct, violations of work rules, or security and privacy incidents
    - Providing and managing access to physical and technical access controls
    - Monitoring activities, access and use to ensure the security and functioning of our systems and assets
    - Securing our offices, premises, and physical assets, including through the use of electronic access systems and video monitoring
- Health and safety: for health and safety purposes, such as contact tracing or including conducting appropriate screenings of Employees prior to entering or accessing certain locations or premises.
- Auditing, accounting, and corporate governance: relating to financial, tax and accounting audits, and audits and assessments of our business operations, security controls, financial controls, or compliance with legal obligations, and for other internal business purposes such as administration of our records retention program.
- Business transactions: relating to planning, due diligence, and implementation of commercial transactions, for example mergers, acquisitions, asset sales or transfers, bankruptcy or reorganization or other similar business transactions.
- Defending and protecting rights: to protect and defend our rights and interests and those of third parties, including to manage and respond to Employee and other legal disputes, to respond to legal claims or disputes, and to otherwise establish, defend or protect our rights or interests, or the rights, interests, health, or safety of others, including in the context of anticipated or actual litigation with third parties.
- Compliance with applicable legal obligations: relating to compliance with applicable legal obligations (such as hiring eligibility, responding to subpoenas and court orders) as well as assessments, reviews, and reporting relating to such legal obligations, including under employment and labor laws and regulations, Social Security, and tax laws, environmental regulations, workplace safety laws and regulations, and other applicable laws, regulations, opinions and guidance.

RETENTION OF PERSONAL INFORMATION

We will retain your personal information, including sensitive personal information, as long as necessary for purposes for which the personal information was collected and is used by us, as stated in this Notice. To the extent permitted by applicable law, we will retain and use your personal information as necessary to comply with our legal obligations, resolve disputes, maintain appropriate business records, and enforce our agreements.

SENSITIVE PERSONAL INFORMATION

Notwithstanding the "Purposes for Collecting and Using Personal Information" section above, we only use and disclose sensitive personal information as reasonably necessary (i) to perform our services requested by you, (ii) to help ensure security and integrity, including to prevent, detect, and investigate security incidents, (iii) to detect, prevent and respond to malicious, fraudulent, deceptive, or illegal conduct, (iv) to verify or maintain the quality and safety of our services, (v) for compliance with our legal obligations, (vi) to our service providers who perform services on our behalf, and (vii) for purposes other than inferring characteristics about you. We do not use or disclose your sensitive personal information other than as authorized pursuant to section 7027 of the CCPA regulations (Cal. Code. Regs., tit. 11, § 7027 (2022)).

CALIFORNIA RESIDENTS' RIGHTS

Employee Rights. In general, California residents have the following rights with respect to their personal information:

- Do not sell or share (opt-out): to opt-out of our sale or sharing of their personal information. We do not sell or share personal information of Employees as defined by CCPA, including about California consumers who we know are younger than 16 years old.
- Right of deletion: to request deletion of their personal information that we have collected about them and to have such personal information deleted (without charge), subject to certain exceptions.
- Right to know: the right to know what personal information we have collected about them, including the categories of personal information, the categories of sources from which the personal information is collected, the business or commercial purpose for collecting, selling, or sharing personal information, the categories of third parties to whom we disclose personal information, and the specific pieces of personal information we have collected about them.
- Right to correct inaccurate information: to request correction of their personal information that we have collected about them and to have such personal information corrected.
- Right to limit the use or disclosure of sensitive personal information: the right to limit the use or disclosure of sensitive personal information to those uses authorized by CCPA. However, we do not use or disclose sensitive personal information except for the purposes described above under "Sensitive Personal Information", as authorized by CCPA.
- Right to non-discrimination: the right not to be subject to discriminatory treatment for exercising their rights under CCPA.
- Financial incentives: California residents have the right to be notified of any financial incentives offers and their material terms, the right to opt-out of such incentives at any time and may not be included in such incentives without their prior informed opt-in consent. Where we offer any financial incentives under the CCPA, we will notify you in advance of the material terms of such incentives and your related rights, before we obtain your consent to such incentives.

Submitting Requests. You may submit requests to us here. In addition, you may make certain requests to us by contacting as at 1-800-332-9978 (toll free).

Please note that we may require additional information from you in order to verify your request.

Authorized agents may submit requests to us here. If you are submitting a request through an authorized agent, the authorized agent must confirm their relationship with you. We may also request that any authorized agents verify their identity, including by providing information about themselves, such as their name, email, phone number, and address. We may reach out to you directly to confirm that you have provided the agent with your permission to submit the request on your behalf.

There may be circumstances where we will not be able to honor your request. For example, if you request deletion, we may need to retain certain personal information to comply with our legal obligations or other permitted purposes. However, we will only use personal information provided in a verifiable consumer request to verify your identity or authority to make the request.

SPECIAL NOTICE TO INTERNATIONAL USERS

As a globally operating company, FCA US may transfer your personal information to the United States and to other jurisdictions where we or our affiliates, suppliers or service providers have operations. As such, your personal information may be accessed, stored, processed, or subject to law enforcement requests in these jurisdictions, which may not have equivalent privacy laws as in your home jurisdiction. We will take steps to ensure that your personal information receives an adequate level of protection in the jurisdictions in which we process it, including through appropriate written data processing terms and/or data transfer agreements.

QUESTIONS

If you have any concerns or questions regarding this Employee Notice or the information practices of the Employee Portal, please contact the FCA Privacy Office at dprivacy@stellantis.com, or your local Human Resources representative.

CHANGES TO THE EMPLOYEE NOTICE

FCA reserves the right to change this Employee Notice from time to time and at its sole discretion. If the Employee Notice changes, the revised policy will be posted at the Employee Notice link on the Employee Portal home page. We will notify Employees if we make a material change to how we handle Employee personal information.