



California Employee Privacy Notice

The California Consumer Privacy Act (“CCPA”) imposes specific obligations on businesses processing personal information of California residents. Pursuant to the CCPA, Sprouts Farmers Market, Inc., together with its subsidiaries (“Company”, “we” or “us”) is required to provide its employees, who are California residents (“California Team Members”) a notice, used at or before the point of collection of such personal information, that identifies the categories of personal information that may be collected and why Company collects such information.

This California Employee Privacy Notice (“Notice”) is intended to provide California Team Members with the CCPA required notice. In the event of any conflict between the terms of this Notice and terms of any other Company policy the terms of this Notice prevail.

1. Updates

This Notice will be updated from time to time to reflect changes in our business, legal or regulatory obligations. Company will not collect additional categories of your personal information or use your personal information already collected for additional purposes without providing you with a notice of our intent to do so. Any changes to this Notice will be effective from the date they are communicated, whether by posting or otherwise.

2. Definitions

- 2.1 “Company” includes Sprouts Farmers Market, Inc., together with its subsidiaries.
- 2.2 “Personal information” has the meaning as defined in the CCPA, and includes information that is collected by Company about you in the course employment for employment related purposes and encompasses any information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with you.
- 2.3 “Process”, “processed” or “processing” means any operation or set of operations which is performed on personal information, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of personal information.
- 2.4 “Team Members”, “Team Member”, “employee”, or “you” means an identified or identifiable natural person who is a California resident and who is acting as a Company job applicant, employee, or contractor. In this context “job applicant” refers to any person who has submitted his or her candidacy with Company; “employee” or “Team Member” refers to any person who is employed at Company as a full-or part-time employee or temporary worker, and “contractor” means a natural person who provides any service to a business pursuant to a written contract.

3. Personal Information We Collect About You

Listed below are the categories of personal information that Company may process about Team Members:

- 3.1 Identifiers, including real name, alias, postal address, unique personal identifiers, email, account name, social security number, driver's license number, passport number or other similar identifiers.
 - 3.1.1 In this context, a "unique personal identifier" means a persistent identifier that can be used to recognize a Team Member, or a device that is linked to a Team Member, over time and across different services, including, but not limited to, a device identifier; an Internet Protocol address; cookies, beacons, pixel tags, mobile ad identifiers, or similar technology; customer number, unique pseudonym, or user alias; telephone numbers, or other forms of persistent or probabilistic identifiers.
- 3.2 Characteristics of Protected Classifications Under California or Federal Law, including the following: race, skin color, national origin, natural hair, ancestry, religion (includes religious dress and grooming practices), sex/gender (includes pregnancy, childbirth, breastfeeding and/ or related medical conditions), gender identity, gender expression, sexual orientation, marital status, medical condition (genetic characteristics, cancer or a record or history of cancer), disability (mental and physical including HIV/AIDS, cancer, and genetic characteristics), genetic information, military or veteran status, request for family care leave, request for leave for a Team Member's own serious health condition, request for pregnancy disability leave, and age.
- 3.3 Biometric Information, including imagery of your iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.
- 3.4 Internet or Other Electronic Network Activity Information, including browsing history, search history and information regarding a Team Member's interaction with an internet website, application or advertisement.
- 3.5 Professional or Employment-related Information, including job related data, maintained as part of the employment relationship that is present in: a job application or resume; an employment contract; a contractor agreement; a performance review; a disciplinary record; photos; biometric data; information from company devices or vehicles; browsing and search history; payroll and benefits related data; internal and external contact information; or information captured from video, audio, systems, or other forms of monitoring or surveillance.
- 3.6 Education Information, including information about a Team Member's educational background, such as education records, report cards, and transcripts that is not publicly available.
- 3.7 Inferences, including any information drawn from any of the personal information categories referenced above to create a profile about a Team Member reflecting the Team Member's preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

4. Purposes for Collecting Your Personal Information

Company collects the personal information identified in Section 3 above for the reasons listed below.

- 4.1 To Recruit Team Members, including to conduct employment related background screening and checks.
- 4.2 To Administer Benefits, such as medical, pension and dental benefits, including recording and processing eligibility of dependents, absence and leave monitoring, insurance and accident management and provision of online total reward information and statements.
- 4.3 To Pay and Reimburse for Expenses, including salary administration, payroll management, payment of expenses, to administer other compensation related payments, including assigning amounts of bonus payments to individuals, administration of departmental bonus pools and administration of stock option payments.
- 4.4 To Conduct Performance-Related Reviews, including performance appraisals, career planning, skills monitoring, job moves, promotions and staff re-structuring.
- 4.5 To Monitor Work-Related Licenses and Credentials, including ensuring compliance, training, examination and other requirements are met with applicable regulatory bodies.
- 4.6 To Provide Our Team Members with Human Resources Management Services, including providing Team Member data maintenance and support services, administration of separation of employment, approvals and authorization procedures, administration and handling of employee claims, and travel administration.
- 4.7 To Administer International Assignments, including relocation services, documenting assignment terms and conditions, obtaining relevant immigration documents, initiating vendor services, fulfilling home/host country tax administration and filing obligations, addressing health requirements and populating the International Mobility global system.
- 4.8 To Maintain Your Contact Information, including altering your details across relevant entities within the Company group of companies (for example personal, other employment and transferring roles).
- 4.9 To Assist You in Case of Emergency, including maintenance of contact details for you, and your dependents in case of personal or business emergency.
- 4.10 To Monitor Eligibility to Work in the U.S., which means monitoring and ensuring compliance of Team Members' ability to work in the U.S.
- 4.11 To Conduct Healthcare-Related Services, including conducting pre-employment and employment-related medical screenings for return to work processes and medical case management needs; determining medical suitability for particular tasks; identifying health needs of Team Members to plan and provide appropriate services, including operation of sickness policies and procedures; providing guidance on fitness for travel and fitness for expatriation; and recording results of specific medical and industrial hygiene tests, commonly known as "health surveillance".
- 4.12 To Facilitate Better Working Environment, which includes conducting staff surveys, providing senior management information about other Team Members, and conducting training.
- 4.13 To Ensure a Safe and Efficient Working Environment, which includes Company actions relating to disciplinary actions, union grievances, code of conduct processes and investigations.
- 4.14 To Maintain Security on Company Websites and Internet Connected Assets, which includes hosting and maintenance of computer systems and infrastructure; management of Company's software and hardware computer assets; systems testing, such as development of new systems and end-user testing of computer systems; training; and monitoring email and Internet access.
- 4.15 To Comply with Applicable Law or Regulatory Requirements, such as legal (state and federal) and internal company reporting obligations, including headcount, management information, demographic and Health, Safety, Security and Environmental reporting.

5. Further Information

If you have any questions about this statement, please contact the Human Resources Department.

Effective 1.1.2020