The Hain Celestial Group, Inc.

PRIVACY POLICY FOR THE EU-U.S. DATA PRIVACY FRAMEWORK, U.K. EXTENSION TO THE EU-U.S. DATA PRIVACY FRAMEWORK AND THE SWISS-U.S. DATA PRIVACY FRAMEWORK

NON-HR PERSONAL DATA

Last modified and effective as of July 18, 2024.

Introduction

This Privacy Policy for the EU-U.S. Data Privacy Framework, U.K. Extension to the EU-U.S. Data Privacy Framework and Swiss-U.S. Data Privacy Framework ("Policy") applies to The Hain Celestial Group, Inc. ("Hain"). Hain receives non-HR Personal Data in the U.S. transferred[1] from the European Economic Area ("EEA"), United Kingdom, and Switzerland related to the categories of Data Subjects and purposes set forth below. To facilitate these transfers in accordance with applicable data protection laws, Hain

- complies with the EU-U.S. Data Privacy Framework ("EU-US DPF"), the U.K. Extension to the EU-US DPF (UK Extension), and the Swiss-U.S. Data Privacy Framework (Swiss DPF) as set forth by the U.S. Department of Commerce ("DOC") regarding the collection, use, disclosure and retention of HR personal data transferred from the European Economic Area ("EEA"), U.K. or Switzerland to the United States, and
- has certified to the DOC that it adheres to the EU-US DPF Principles and Swiss DPF Principles ("Principles").

This privacy policy ("Policy") outlines our general policies and practices for implementing the EU-US DPF Principles and Swiss DPF Principles (collectively, "Principles") and our commitment to subject all non-HR Personal Data received in reliance on the EU-U.S. DPF, UK Extension, or Swiss DPF to the Principles. This Policy should be read in conjunction with the Hain Privacy Policy.

Please note that we may amend this Policy at any time, including as required and consistent with the Principles. If there is any conflict between the terms of this Policy and the Principles, the Principles shall govern. We will post notice of material changes on the top of this Policy, on our website homepage, or in our website privacy policy. Material changes will apply to non-HR Personal Data we collect or receive prior to the change unless they reduce the rights of the individuals whose non-HR Personal Data is impacted or are inconsistent with the Principles.

[1] For purposes of cross border transfers, a transfer includes a transmittal of Personal Data to Hain in the U.S. from the EU, UK, or Switzerland or access by Hain in the U.S. to data stored in a server in the EU, UK or Switzerland.

To view our certification on the Data Privacy Framework List, please visit Participant Search (dataprivacyframework.gov). To learn more about the EU-US DPF, UK Extension, and Swiss DPF Program, please visit Home (dataprivacyframework.gov). Hain is subject to the investigatory and enforcement powers of the U.S. Federal Trade Commission ("FTC").

If you have questions or would like additional information, please contact us at:

Hain Celestial Group, Inc.
12th Floor
221 River Street
Hoboken, NJ 07030

Email: HCGUS.DataPrivacy@hain.com

Definitions

For the purpose of this Policy, the following definitions apply:

"**Data Subject"** means the individual to whom the non-HR Personal Data relates.

"**Personal Data"** means any information relating to an identified or identifiable natural person (i.e., Data Subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

"Process" or "**Processing"** means any operation performed on Personal Data 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.

"Special Category Data" or "**Sensitive Data"** means Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. For Personal Data transferred from Switzerland only, this also includes information on social security measures or administrative or criminal proceedings and sanctions, which are treated outside pending proceedings.

Notice

Purpose of Collection

Hain may receive and processes non-HR Personal Data for purposes related to the following:

- respond to your questions and requests, including consumer complaints,
- combine all the information we collect or receive about you for any of the foregoing purposes,
- communicate with you about your account and other matters, and in our discretion, changes to any Hain policy that may affect you,
- conduct research and analysis related to, and manage and improve, our websites, mobile applications, products, services, advertising, ecommerce product listings, promotions and sales, and understand how you interact with us through social media platforms, including,

for example, to make our websites and mobile applications easier to use with better content by understanding how people use our websites, mobile applications, products and services and engage with us using social media and advertising,
- help you locate stores near you that sell our products,
- Establishing and administering business relationships
- implement other activities disclosed at the time you provide your information,
- implement social networking features you have activated, and/or
- manage online communities for the sharing and exchange of reviews, comments, feedback, ideas, and other user generated content,
- personalize your website experience through tailored content, ads and offers,
- process transactions and ship products to you,
- provide you with information about our company, products, services, promotions and other special offers, including through the delivery of targeted advertising,
- review ad performance, delivery verification and measurement,
- and to the extent that you provide us with financial information in connection with shopping or commercial services, we will use the financial information to process orders and bill you for products and/or services. By submitting your account or credit or debit card number and related personal information, you are authorizing Hain to give that information to our service providers and the merchant and credit card company for order confirmation and fulfillment, identity verification and managing risk and fraud.

Categories of Data Subjects

Hain receives non-HR Personal data transferred from the EEA, United Kingdom, or Switzerland that relates to Hain customers, clients, business partners, distributors, vendors and service providers, and visitors.

Categories of Personal Data

The categories of non-HR Personal Data transferred to the U.S. may include but are not limited to contact details such as name, email address, IP address, mailing address, contact person, other contact information, date of birth, financial information including but not limited to debit or credit card number, contract data , product-related incident information, demographic information such as age and gender, commercial information such as browsing habits, interactions, and purchasing history, geographic location data such as country, city and postal code, and employment and education information.

How We Use Personal Data

In general, we use the non-HR Personal Data we receive only for the purpose it was collected, for compatible purposes, as permitted or required by law, as necessary to carry out our contractual duties and obligations, and as otherwise provided in this Policy, in other relevant privacy notices, our website privacy policy or in accordance with the Principles. For example, we use non-HR Personal Data for the following purposes:

- Processing, managing, and responding to Data Subject requests for information, assistance, or for product or services orders.

- Entering into and managing contracts and agreements.

- Communicating with Data Subjects.
- Protecting against and preventing fraud and illegal activity.
- Protecting our interests and legal rights; investigating allegations; responding to subpoenas; exercising, establishing or defending legal claims.
- For other everyday business purposes including security, IT and website administration, corporate governance, auditing, human capital analytics, and reporting obligations.
- To respond to lawful requests from public authorities including to meet national security, public interest or law enforcement requirements.
- As necessary, to comply with our regulatory or legal obligations or operational needs.
- To comply with the Principles.

Disclosures

In general, we do not sell, trade or otherwise disclose non-HR Personal Data transferred to us from the EEA, UK or Switzerland to unaffiliated third parties except with the Data Subject's consent and/or as described in this Policy, our website privacy policy, relevant privacy notices or as required or permitted by law or the Principles. We may disclose non-HR Personal Data for the same reasons that we may use it as described in the policies or notices referenced above, which includes disclosing it to our affiliates and non-affiliated entities as we deem necessary to carry out those purposes. The categories of third parties to whom we may disclose non-HR Personal Data include, but are not limited to:

- Third party controllers including legal counsel; consultants; insurers; investigators; parties to an investigation, claim or controversy; business partners, or professional services providers (e.g., accountants, attorneys).
- Third parties as you direct.
- Third party processors or agents who perform services on our behalf pursuant to our written instructions (e.g., payment processors, data storage providers, IT and software service providers, shipping and fulfillment services, advertising and marketing vendors).
- Government agencies, law enforcement, courts, mediators or arbitrators. We may disclose Personal Data in response to lawful requests by public authorities including to meet national security or law enforcement requirements.
- Third parties in connection with certain business transactions such as a sale, acquisition, merger, or change in control, or in preparation for any of these events. In such cases, we will take appropriate steps under the circumstances and to the extent possible to ensure that the recipient agrees to provide privacy protections substantially similar to those established by this Policy. Any entity that acquires all or substantially all of our assets will have the right to continue using your data consistent with this Policy or as otherwise agreed to by the Data Subject.

We may disclose or make public aggregate, de-identified or anonymized data derived from non-HR Personal Data. Such information, however, will not identify the Data Subject or any other individual.

Principles

Notice

We provide notice to Data Subjects through this Policy, our website privacy policy or other forms of communications or notices regarding the collection, processing, and disclosure of their Personal Data including their rights and our adherence to the Principles.

Choice

Prior to disclosing non-HR Personal Data to a third party, other than a third party acting as an agent pursuant to our written instructions on our behalf, and prior to using that non-HR Personal Data for a purpose materially different from the one for which it was originally collected or subsequently authorized, we will permit Data Subjects to *opt out* of such disclosure (as required by applicable law).

Prior to disclosing Special Category or Sensitive Data to a third party, or prior to using such data for a purpose different from the one for which it was originally collected or subsequently authorized, we will permit the Data Subject to affirmatively and explicitly *opt-in* to such disclosure (as required by applicable law). Please note the Data Subject's affirmative consent is not required for us to disclose this data when it is in their vital interests or that of another person; as necessary for the establishment of legal claims or defenses; for purposes of providing medical care or diagnosis; or as it relates to data the Data Subject has manifestly made public.

Accountability for Onward Transfer

We may transfer non-HR Personal Data onward to third party controllers and/or processors, as noted in the section on Disclosures, for the purpose(s) stated in this Policy and other relevant policies or notices, in accordance with the Notice and Choice Principles, and pursuant to a written contract.

Hain will remain liable for the failure of a third party processor to comply with the Principles unless we are able to demonstrate that we are not responsible for the event giving rise to the damage.

We endeavor to choose affiliates and non-affiliate companies with similar standards to ours regarding the protection of Personal Data and who are either subject to a law providing an adequate level of privacy protection or have agreed to provide an adequate level of protection. These companies are generally not authorized to use the information we disclose to them for any other purpose.

Security

Hain takes reasonable and appropriate physical, technical, and administrative measures to protect the non-HR Personal Data we receive to guard against loss, misuse or unauthorized access, disclosure, alteration or destruction. However, no system for safeguarding Personal Data or other information is 100% secure and although we have taken steps to protect Personal Data, we cannot fully eliminate security risks associated with Personal Data.

Data Integrity and Purpose Limitation

We take reasonable and appropriate steps to limit the collection of non-HR Personal Data to that which is relevant to accomplish the purpose(s) disclosed to the Data Subject and for compatible purposes.

To the extent necessary to achieve those purposes, Hain will take reasonable steps to ensure the non-HR Personal Data is reliable for its intended use, accurate, complete, and current.

We retain non-HR Personal Data in an identifiable form only for the period necessary to fulfil the purposes of the processing, unless a longer retention period is required or permitted by law or the Principles. We will adhere to the Principles for as long as we retain the non-HR Personal Data collected under the EU-US DPF, UK Extension, or Swiss DPF.

Access

Data Subjects have rights relating to the non-HR Personal Data we maintain about them, subject to certain limitations. These rights include the following:

- To access or request a copy of their Personal Data.
- To correct, amend, or delete their Personal Data where it is inaccurate or has been processed in violation of the Principles.

To exercise any of these rights, please contact us at: HCGUS.DataPrivacy@hain.com.

Data Subjects must provide adequate identification to verify their identity and/or assist us in searching for their Personal Data. We may deny or limit a request if providing access would be unreasonably burdensome or expensive, the rights of non-requesting individuals would be adversely affected, or the individual is unable to present appropriate identification to verify their identity.

Recourse, Enforcement and Liability

Hain is committed to resolving complaints arising out of the processing of non-HR Personal Data in accordance with the Principles. You may submit a complaint to us by emailing us at HCGUS.DataPrivacy@hain.com.

In the event we are unable to satisfactorily resolve your complaint, you may contact VeraSafe to assist you in resolving your complaint at https://verasafe.com/privacy-solutions/data-privacy-framework-dispute-resolution-program/.

Data Subjects may invoke binding arbitration to address any alleged violation of our obligations under the Principles that remains fully or partially unremedied after utilizing independent dispute resolution ("Residual Claims"). Arbitral decisions will be binding on all parties to the arbitration. A Data Subject must take the following steps prior to initiating an arbitration claim: (1) raise the claimed violation directly with Hain and allow us an opportunity to resolve the issue within 45 days; (2) use the designated independent recourse mechanism to resolve the issue; and (3) raise the issue to the Department of Commerce through the Data Subject's Data Protection Authority and afford the Department of Commerce the opportunity to resolve the issue. Please follow this link for additional information ANNEX I (introduction) (dataprivacyframework.gov).

Contact Information

Please contact the Hain data protection coordinator at HCGUS.DataPrivacy@hain.com with any questions.

Hain Celestial Group, Inc.
12th Floor
221 River Street
Hoboken, NJ 07030