The Procter & Gamble Company

Data Privacy Framework: Consumer Privacy Policy

Last Updated: July 10, 2024

The Procter & Gamble Company and its U.S. subsidiaries and affiliates identified in Exhibit 1 (collectively, "P&G") respect your concerns about privacy.

P&G participates in the EU-U.S. Data Privacy Framework (EU-U.S. DPF), the UK Extension to the EU-U.S. DPF and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) (collectively, the "DPF") administered by the U.S. Department of Commerce. P&G commits to comply with the DPF Principles with respect to Consumer Personal Data the company receives from the EU, United Kingdom and Switzerland in reliance on the DPF. This Policy describes how P&G implements the Data Privacy Framework Principles for Consumer Personal Data. If there is any conflict between the terms in this Policy and the EU-U.S. DPF Principles and/or the Swiss-U.S. DPF Principles, the Data Privacy Framework Principles shall govern. The definitions used in this Policy apply only with respect to this Policy and P&G's Data Privacy Framework certification.

"Consumer" means any natural person who is located in the EU, UK or Switzerland, but excludes any individual acting in his or her capacity as a Worker.

"Controller" means a person or organization which, alone or jointly with others, determines the purposes and means of the processing of Personal Data.

"Data Privacy Framework Principles" or **"DPF Principles**" means the Principles and Supplemental Principles of the DPF.

"EU" means the European Union and Iceland, Liechtenstein and Norway.

"Personal Data" means any information, including Sensitive Data, that is (i) about an identified or identifiable individual, (ii) received by P&G in the U.S. from the EU, UK or Switzerland, and (iii) recorded in any form.

"Processor" means any natural or legal person, public authority, agency or other body that processes Personal Data on behalf of a Controller.

"Sensitive Data" means Personal Data specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (including trade union-related views or activities), sex life (including personal sexuality), information on social security measures, the commission or alleged commission of any offense, any proceedings for any offense committed or alleged to have been committed by the individual or the disposal of such proceedings or the sentence of any court in such proceedings (including administrative proceedings and criminal sanctions).

"**UK**" means the United Kingdom (and Gibraltar).

"Worker" means any current, former or prospective employee, contractor, intern or temporary worker of P&G or any of its EU, UK or Swiss subsidiaries or affiliates, or any related individual whose Personal Data P&G processes in connection with an employment relationship, who is located in the EU, UK or Switzerland.

P&G's certification to the Data Privacy Framework program, along with additional information about the Data Privacy Framework Program, can be found at https://www.dataprivacyframework.gov/. For more information about P&G's processing of Consumer Personal Data with respect to information collected on its website, please visit P&G's Global Consumer Privacy Policy at https://privacypolicy.pg.com/en/.

Types of Personal Data P&G Collects

P&G obtains Personal Data about Consumers in various ways. For example, P&G collects Personal Data directly from Consumers when they interact with P&G's website and mobile apps (collectively, the "Services"). The company may use this information for the purposes indicated in P&G's Global Consumer Privacy Policy.

The types of Personal Data P&G collects about Consumers include:

- contact information (such as name (including nickname, alias and previous names), title, email address, mailing address and telephone number);
- personal characteristics and preferences (such as age range, marital and family status, shopping preferences, languages spoken, loyalty and rewards program data, household demographic data, data from social media platforms, education and professional information, hobbies and interests and propensity scores from third parties (likelihood of purchase, experiencing a life event, etc.);
- transaction and commercial information (such as customer account information, qualification data, purchase history and related records, records related to downloads and purchases of products and applications, non-biometric data collected for consumer authentication (passwords, account security questions) and customer service records);
- unique IDs and account details (such as customer number, account number, subscription number, rewards program number), system identifiers (including username or online credentials), device advertisers, advertising IDs and IP address;
- online & technical information such as (such as IP address, MAC address, SSIDs or other device identifiers or persistent identifiers, online user ID, encrypted password, device characteristics (such as browser information), web server logs, application logs, browsing data, viewing data (TV, streaming), website and app usage, first party cookies, third party cookies, flash cookies, Silverlight cookies, web beacons, clear gifs and pixel tags);
- precise geolocation (such as latitude/longitude);
- health-related information (such as general health and symptom information, pregnancy-related information or information about physical or mental health, disease state, medical history or medical treatment or diagnosis, medicines taken and related information);

- financial information (such as bank account number and details and payment card information);
- government-issued ID or tax ID;
- audio and visual information (such as photographs, video images, CCTV recordings, call center recordings and call monitoring records and voicemails);
- smart devices and sensor data (such as smart device records, IoT products);
- data about households or children (such as the number of children you have, your children's diaper sizes, their genders and ages);
- biometric data (such as facial recognition data and a mathematical representation of your biometric identifier); and
- information derived from other information listed in this section.

In addition, P&G obtains Personal Data, such as contact information and financial accounts of representatives of its vendors (such as payment processors and shipping carriers). P&G uses this information to manage its relationships with these parties, process payments and carry out P&G's contractual obligations.

P&G also may obtain and use Consumer Personal Data in other ways for which P&G provides specific notice at the time of collection.

P&G's privacy practices regarding the processing of Consumer Personal Data comply with the Data Privacy Framework Principles of Notice; Choice; Accountability for Onward Transfer; Security; Data Integrity and Purpose Limitation; Access; and Recourse, Enforcement and Liability.

Notice

P&G provides information in this Policy and the company's Global Consumer Privacy Policy about its Consumer Personal Data practices, including the types of Personal Data P&G collects, the types of third parties to which P&G discloses the Personal Data and the purposes for doing so, the rights and choices Consumers have for limiting the use and disclosure of their Personal Data and how to contact P&G about its practices concerning Personal Data.

Relevant information also may be found in notices pertaining to specific data processing activities.

Choice

P&G generally offers Consumers the opportunity to choose whether their Personal Data may be (i) disclosed to third-party Controllers or (ii) used for a purpose that is materially different from the purposes for which the information was originally collected or subsequently authorized by the relevant Consumer. To the extent required by the Data Privacy Framework Principles, P&G obtains opt-in consent for certain uses and disclosures of Sensitive Data. Consumers may contact P&G as indicated below regarding the company's use or disclosure of their Personal Data. Unless P&G offers Consumers an appropriate choice, the company uses Personal Data only for purposes that are materially the same as those indicated in this Policy.

Sharing of Consumer Personal Data

This Policy and P&G's Global Consumer Privacy Policy describe P&G's sharing of Consumer Personal Data.

P&G shares Consumer Personal Data with its affiliates and subsidiaries, which may include any entity within the P&G network of companies, for purposes of operating P&G's business and providing P&G products and services. P&G also may share Consumer Personal Data with third-party Processors the company retains to perform services on its behalf, such as payment processing and authorization, order fulfillment, transportation, customs clearance, marketing, data analytics, customer support and fraud prevention. These third-party Processors may use Consumer Personal Data only on P&G's behalf and pursuant to P&G's instructions, for the purpose of providing services to P&G such as those described above. P&G may disclose Consumer Personal Data without offering an opportunity to opt out, and may be required to disclose the Personal Data, (i) to third-party Processors the company has retained to perform services on its behalf and pursuant to its instructions, (ii) if it is required to do so by law or legal process, or (iii) in response to lawful requests from public authorities, including to meet national security, public interest or law enforcement requirements. P&G also reserves the right to transfer Personal Data in the event of an audit or if the company sells or transfers all or a portion of its business or assets (including in the event of a merger, acquisition, joint venture, reorganization, dissolution or liquidation).

Accountability for Onward Transfer of Personal Data

This Policy and P&G's Global Consumer Privacy Policy describe P&G's sharing of Consumer Personal Data.

Except as permitted or required by applicable law, P&G provides Consumers with an opportunity to opt out of sharing their Personal Data with third-party Controllers. P&G requires third-party Controllers to whom it discloses Consumer Personal Data to contractually agree to (i) only process the Personal Data for limited and specified purposes consistent with the consent provided by the relevant Consumer, (ii) provide the same level of protection for Personal Data as is required by the Data Privacy Framework Principles, and (iii) notify P&G and cease processing Personal Data (or take other reasonable and appropriate remedial steps) if the third-party Controller determines that it cannot meet its obligation to provide the same level of protection for Personal Data as is required by the Data Privacy Framework Principles.

With respect to transfers of Consumer Personal Data to third-party Processors, P&G (i) enters into a contract with each relevant Processor, (ii) transfers Personal Data to each such Processor only for limited and specified purposes, (iii) ascertains that the Processor is obligated to provide the Personal Data with at least the same level of privacy protection as is required by the Data Privacy Framework Principles, (iv) takes reasonable and appropriate steps to ensure that the Processor effectively processes the Personal Data in a manner consistent with P&G's obligations under the Data Privacy Framework Principles, (v) requires the Processor to notify P&G if the Processor determines that it can no longer meet its obligation to provide the same level of protection as is required by the Data Privacy Framework Principles, (vi) upon notice, including under (v) above, takes reasonable and appropriate steps to stop and remediate unauthorized processing of the Personal Data by the Processor, and (vii) provides a summary or representative copy of the relevant

privacy provisions of the Processor contract to the Department of Commerce, upon request. P&G remains liable under the Data Privacy Framework Principles if the company's third-party Processor onward transfer recipients process relevant Personal Data in a manner inconsistent with the Data Privacy Framework Principles, unless P&G proves that it is not responsible for the event giving rise to the damage.

Security

P&G takes reasonable and appropriate measures to protect Consumer Personal Data from loss, misuse and unauthorized access, disclosure, alteration and destruction, taking into account the risks involved in the processing and the nature of the Personal Data.

Data Integrity and Purpose Limitation

P&G limits the Consumer Personal Data it processes to that which is relevant for the purposes of the particular processing. P&G does not process Consumer Personal Data in ways that are incompatible with the purposes for which the information was collected or subsequently authorized by the relevant Consumer. In addition, to the extent necessary for these purposes, P&G takes reasonable steps to ensure that the Personal Data the company processes is (i) reliable for its intended use, and (ii) accurate, complete and current. In this regard, P&G relies on its Consumers to update and correct the relevant Personal Data to the extent necessary for the purposes for which the information was collected or subsequently authorized. Consumers may contact P&G as indicated below to request that P&G update or correct relevant Personal Data.

Subject to applicable law, P&G retains Consumer Personal Data in a form that identifies or renders identifiable the relevant Consumer only for as long as it serves a purpose that is compatible with the purposes for which the Personal Data was collected or subsequently authorized by the Consumer.

Access

Consumers generally have the right to access their Personal Data. Accordingly, where appropriate, P&G provides Consumers with reasonable access to the Personal Data P&G maintains about them. P&G also provides a reasonable opportunity for those Consumers to correct, amend or delete the information where it is inaccurate or has been processed in violation of the Data Privacy Framework Principles, as appropriate. P&G may limit or deny access to Personal Data where the burden or expense of providing access would be disproportionate to the risks to the Consumer's privacy in the case in question, or where the rights of persons other than the Consumer would be violated. Consumers may request access to their Personal Data by contacting P&G as indicated below.

Recourse, Enforcement and Liability

P&G has mechanisms in place designed to help assure compliance with the Data Privacy Framework Principles. P&G conducts an annual self-assessment of its Consumer Personal Data practices to verify that the attestations and assertions P&G makes about its Data Privacy

Framework privacy practices are true and that P&G's privacy practices have been implemented as represented and in accordance with the Data Privacy Framework Principles.

In compliance with the Data Privacy Framework, P&G commits to resolve Data Privacy Framework Principles - related complaints about P&G's collection and use of Consumer Personal Data. Consumers with inquiries or complaints regarding P&G's handling of Personal Data received in reliance on Data Privacy Framework Principles should first contact P&G as specified below.

P&G will take steps to remedy issues arising out of its alleged failure to comply with the Data Privacy Framework Principles.

If a Consumer's complaint cannot be resolved through P&G's internal processes, P&G will cooperate with JAMS pursuant to the JAMS Data Privacy Framework Program, which is described on the JAMS website at https://www.jamsadr.com/eu-us-data-privacy-framework. JAMS mediation may be commenced as provided for in the JAMS rules. The services of JAMS are provided at no cost to the Consumer. Following the dispute resolution process, the mediator or the Consumer may refer the matter to the U.S. Federal Trade Commission, which has investigatory and enforcement powers over P&G. Under certain circumstances, Consumers also may be able to invoke binding arbitration to address complaints about P&G's compliance with the Data Privacy Framework Principles.

How to Contact P&G

To contact P&G with questions or concerns about this Policy or P&G's Consumer Personal Data practices:

The Procter & Gamble Company
Attn: Data Protection Officer
1 Procter & Gamble Plaza
Cincinnati, OH 45202

E-mail: pgprivacyofficer.im@pg.com

Exhibit 1

List of P&G U.S. entities certifying to the Data Privacy Framework

The Procter & Gamble Company
1837, LLC
Agile Pursuits Franchising, Inc.
Agile Pursuits, Inc.
Celtic Insurance Company, Inc.
Charlie Banana (USA), LLC
Farmacy Beauty, LLC
First Aid Beauty Limited
Fountain Square Music Publishing Co., Inc.
Gillette Commercial Operations North America
Gillette Holding Company LLC
Gillette Management, LLC
Grooming Ventures - FL LLC
Grooming Ventures LLC
Liberty Street Music Publishing Company, Inc.
Mielle Organics, LLC
Mielle, Inc.
Oral-B Laboratories
P&G Hair Care Holding, Inc.
Procter & Gamble Commercial LLC
Procter & Gamble do Brazil, LLC
Procter & Gamble Eastern Europe, LLC
Procter & Gamble Energy Company LLC
Procter & Gamble Far East, Inc.
Procter & Gamble Hair Care, LLC
Procter & Gamble Holding LLC
Procter & Gamble India Holdings, Inc.
Procter & Gamble Leasing LLC
Procter & Gamble Mexico (US) LLC
Procter & Gamble Productions, Inc.
Procter & Gamble RHD, Inc.
Proof Company, LLC
Redmond Products, Inc.
Richardson-Vicks Real Estate Inc.
Riverfront Music Publishing Co., Inc.
Rosemount LLC
Shulton, Inc.
Sunflower Distributing LLC
Tambrands Inc.

TAOS - FL, LLC
The Dover Wipes Company
The Gillette Company LLC
The Procter & Gamble Distributing LLC
The Procter & Gamble Global Finance Company, LLC
The Procter & Gamble Manufacturing Company
The Procter & Gamble Paper Products Company
The Procter & Gamble U.S. Business Services Company
This is L. Inc.
Tula Life, Inc.
United Beauty Brands, LLC
US CD LLC
Walker & Co. Brands, Inc.
Zenlen, Inc.