The Procter & Gamble Company

Data Privacy Framework: Worker Privacy Policy

Last Updated: August 21, 2023

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. This Policy describes how P&G implements the Data Privacy Framework Principles for Worker 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.

"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 (1) about an identified or identifiable individual, (2) received by P&G in the U.S. from the EU, UK or Switzerland, and (3) 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, intern, temporary worker or contractor of P&G or any of its EU, UK or Swiss 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 Data Privacy Framework certification, along with additional information about the Data Privacy Framework, can be found at https://www.dataprivacyframework.gov/.

Types of Personal Data P&G Collects

P&G collects Personal Data about Workers to carry out and support human resources functions and activities, including: (1) recruiting and hiring job applicants; (2) managing Worker communications and relations; (3) providing compensation and benefits, including salary planning; (4) administering payroll; (5) providing corporate credit cards and processing corporate expenses and reimbursements; (6) managing Worker participation in human resources plans and programs; (7) carrying out obligations under employment contracts; (8) managing Worker performance, staffing, career development and recognition (including delivery of gifts); (9) conducting training and talent development; (10) facilitating Worker relocations and international assignments; (11) managing Worker headcount, time and attendance and office allocation; (12) managing the Worker termination process; (13) managing information technology and communications systems, such as the corporate email system, electronic devices and the company directory; (14) conducting ethics and disciplinary investigations; (15) administering Worker grievances and claims; (16) managing audit and compliance matters; (17) managing physical and cyber security controls, including physical site access; (18) managing diversity, equality and inclusion efforts, including affinity group membership; (19) facilitating health-related screenings and medical programs (including related to COVID-19); (20) complying with applicable legal obligations, including government reporting, banking and Know-Your-Customer requirements, tax reporting and specific local law requirements; and (21) other general security and human resources purposes, including purposes related to trade union membership. P&G also may obtain and process Personal Data about Workers' emergency contacts and other individuals (such as spouse, family members, dependents and beneficiaries) to the extent Workers provide such information to P&G. P&G processes this information to comply with its legal obligations and for benefits administration and other internal administrative purposes.

The types of Worker Personal Data P&G collects in connection with these activities includes:

- name;
- contact information, such as residential and mailing address, email address and telephone number;
- date and place of birth;
- gender;
- marital status and family or household composition;
- information about children, dependents or other beneficiaries of Workers;
- government-issued identification information, passport or visa information, social security number, driver license, etc.;
- citizenship, residency and nationality information;
- demographic information (such as race, ethnicity, sexual orientation, gender identity, disability status, political views, religious or philosophical beliefs);
- country of birth;
- educational history;
- employment and military history;
- legal work eligibility status;

- criminal history;
- information about job performance, compensation, disciplinary and grievance records and training;
- information about professional licenses, certifications, memberships and affiliations;
- trade union membership;
- financial account information and payment card information;
- information relating to physical or mental health conditions or examinations;
- genetic data (where legally required in connection with an occupational health examination);
- digital signatures, electronic identification data, cookie data, logs and records regarding Worker access to and use of P&G devices and the P&G network, and similar electronic information;
- CCTV footage and other information collected by P&G physical security systems;
- biometric data (such as fingerprints or facial scans);
- photographs, videos and voice recordings; and
- other information Workers may provide.

P&G also may obtain and use Worker 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 Worker 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 notifies Workers about its privacy practices, including the purposes for which it collects and uses Personal Data, 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 Workers have for limiting the use and disclosure of their Personal Data and how to contact P&G about its practices concerning Personal Data. Information regarding P&G's Worker Personal Data practices is contained in this Policy and in P&G's Global Employee Privacy Policy, which is available **here.**

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

Choice

P&G generally offers Workers the opportunity to choose whether their Personal Data may be (1) disclosed to third-party Controllers or (2) used for a purpose that is materially different from the purposes for which the information was originally collected or subsequently authorized by the relevant Worker. To the extent required by the Data Privacy Framework Principles, P&G obtains opt-in consent for certain uses and disclosures of Sensitive Data. Unless P&G offers Workers an appropriate choice, the company uses Personal Data only for purposes that are materially the same as those indicated in this Policy. To exercise their choices, Workers may contact P&G as indicated in this Policy. To the extent and for the period necessary to avoid prejudicing the ability of the company in making promotions, appointments, or other similar employment decisions, P&G is not required to offer notice or choice to Workers.

Sharing of Worker Personal Data

P&G shares Worker 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, and to carry out and support human resources functions and activities. P&G may also share Worker Personal Data with third-party Processors the company retains to perform services on its behalf, such as security, travel, payroll, benefits and other human resources-related activities. Such third-party Processors may use P&G Worker 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 Worker Personal Data without offering an opportunity to opt out, and may be required to disclose the Personal Data, (1) to third-party Processors the company has retained to perform services on its behalf and pursuant to its instructions, (2) if it is required to do so by law or legal process, or (3) 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 describes P&G's sharing of Personal Data.

Except as permitted or required by applicable law, P&G provides Workers 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 Worker Personal Data to contractually agree to (1) only process the Personal Data for limited and specified purposes consistent with the consent provided by the relevant Worker, (2) provide the same level of protection for Personal Data as is required by the Data Privacy Framework Principles, and (3) 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 as is required by the Data Privacy Framework Principles. P&G is not required to enter into a contract to transfer Personal Data to certain third-party Controllers for occasional employment-related operational needs of the company, such as booking flights or hotel rooms or handling insurance coverage.

With respect to transfers of Worker Personal Data to third-party Processors, P&G (1) enters into a contract with each relevant Processor, (2) transfers Personal Data to each such Processor only for limited and specified purposes, (3) 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, (4) 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, (5) 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, (6) upon notice, including under (5) above, takes reasonable and appropriate steps to stop and remediate unauthorized processing of the Personal Data by the Processor, and (7) 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 the 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 Worker 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 Worker Personal Data it processes to that which is relevant for the purposes of the particular processing. P&G does not process Worker Personal Data in ways that are incompatible with the purposes for which the information was collected or subsequently authorized by the relevant Worker. In addition, to the extent necessary for these purposes, P&G takes reasonable steps to ensure that the Personal Data the company processes is (1) reliable for its intended use, and (2) accurate, complete and current. In this regard, P&G relies on its Workers to update and correct Personal Data to the extent necessary for the purposes for which the information was collected or subsequently authorized by the Workers. Workers may contact P&G as indicated in this Policy to request that P&G update or correct relevant Personal Data.

Subject to applicable law, P&G retains Worker Personal Data in a form that identifies or renders identifiable the relevant Worker 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 Worker.

Access

Workers generally have the right to access their Personal Data. Accordingly, where appropriate, P&G provides Workers with reasonable access to the Personal Data P&G maintains about them. P&G also provides a reasonable opportunity for Workers 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 Worker's privacy in the case in question, or where the rights of persons other than the Worker would be violated.

Workers may request access to their Personal Data by contacting P&G as indicated in this Policy.

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 Worker 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 Worker Personal Data. Workers 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.

If a Worker's complaint cannot be resolved through P&G's internal processes, P&G commits to cooperate and comply respectively with the advice of the panel established by the EU data protection authorities (DPAs), the UK Information Commissioner's Office (ICO) and the Gibraltar Regulatory Authority (GRA) and the Swiss Federal Data Protection and Information Commissioner (FDPIC), as appropriate, to address relevant Worker complaints and provide Workers with appropriate recourse free of charge. Under certain circumstances, individuals also may be able to invoke binding arbitration to address complaints about P&G's compliance with the Data Privacy Framework Principles. P&G also is subject to the investigatory and enforcement powers of the U.S. Federal Trade Commission.

How to Contact P&G

To contact P&G with questions or concerns about this Policy or P&G's Worker Personal Data practices, write to or call:

Global Data Protection Officer
1 Procter & Gamble Plaza
Cincinnati, OH 45202
(513) 622-0103
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.
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.
Oral-B Laboratories
P&G Hair Care Holding, Inc.
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 India Holdings, Inc.
Procter & Gamble Leasing LLC
Procter & Gamble Mexico (US) LLC
Procter & Gamble Productions, Inc.
Procter & Gamble RHD, Inc.
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 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
US CD LLC