ALL BRANDS, ONE POLICY TO PROTECT YOU.

Data you share.

We collect information that you share with us through ou
brand experiences as well as information you have provided
who share that data with us. You can control your data

PRIVACY POLICY

Updated August 28, 2025

Download a copy of this Privacy Policy (PDF)

FAQ

Commonly asked questions about how we collect, store and use your personal data, as defined in applicable laws.

Do we sell your personal data for monetary compensation?

No

Do we disclose your personal data to third-party partners?

Yes, where we have a lawful basis to do so.

Do we receive personal data from other companies you have given permission to?

Yes

Do we use your personal data for better product recommendations and site experiences?

Yes, where we have a lawful basis to do so.

Do we give you control of your personal data?

Yes

How You Control Your Personal Data

You are in control of your personal data. You can exercise your rights and change your preferences anytime.

Data Subject Rights Requests

Depending on your location (the jurisdiction in which you are a resident), you may have different data subject rights available to you. These may include requests for access, erasure, rectification/correction, to opt out of receiving marketing emails or texts, object to our use of your email address or phone number for advertising, etc. To submit a Data Subject Rights requests for your jurisdiction, click here.

You can also tell us to stop sending you email and text messages by following the opt-out instructions sent with these communications. Please be aware that we may need to keep certain information to honor your choices (e.g., if you tell us to stop sending marketing emails, we will need your email address on file so that our systems remember that you no longer wish to receive marketing communications to that email address).

Also, there are some situations where we may be unable to grant your request (e.g., deleting transaction data where we have a legal obligation to keep it, or for fraud prevention, security, or to protect the privacy of others, or for the establishment, exercise, or defense of legal claims, among other things).

Traditional Online Behavioral Advertising

How you exercise choice as to interest-based ads

Advertising Industry Opt-Outs

For the U.S., to exercise choice with respect to interest-based advertising, you can utilize the opt-out mechanism provided by the Digital Advertising Alliance ("DAA") by clicking here (for browsers) or here (for app-based opt-outs).

The Network Advertising Initiative ("NAI") has developed a tool that allows consumers to opt out of certain Interest-based Ads delivered by NAI members' ad networks. To learn more about opting out of such targeted advertising or to use the NAI tool, see http://www.networkadvertising.org/choices/.

For Europe, you may click here to learn more about the DAA-Europe's opt-out program.

For Canada, you may click here to learn more about the DAA Canada's opt-out program.

To opt-out of Unified ID 2.0 globally click here.

Online Platform Opt-Outs

P&G may share identifiers connected to you, such as a hashed version of your email address, with online platforms, including but not limited to those listed below, for the purpose of sending you interest-based advertising. To learn more about how these platforms may use your data and about how you can control the use of this data, please follow the links below.

- Google
- Meta
- Microsoft / Bing
- Pinterest
- Reddit
- Snap
- TikTok

Please be aware that, even if you opt-out of certain kinds of interest-based ads, you may continue to receive other ads. Further, opting out of one or more NAI or DAA members only means that those selected members should no longer under the DAA / NAI rules deliver certain targeted ads to you. This will affect services provided by the applicable DAA / NAI members but does not mean you will no longer receive any targeted content and/or ads from non-

participating parties. Also, if your browsers are configured to reject cookies when you visit the opt-out page, or you subsequently erase your cookies, use a different Device or web browser(s), or use a non-browser-based method of access, your DAA / NAI browser-based opt-out may not, or may no longer, be effective. Mobile device opt-outs will not affect browser-based Interest-based ads even on the same device, and you must opt-out separately for each device. We are not responsible for the effectiveness of, or compliance with, any third party opt-out options or programs or the accuracy of their statements regarding their programs.

You can also prevent or reduce getting interest-based ads on websites by declining cookies in your browser(s), or on mobile devices by declining the "access to data" requests that apps usually present when you install them or by adjusting the ad tracking settings on your device.

Please note that you may also receive personalized ads based on your email address or phone number, if you have provided those to us for marketing purposes. To opt out of that usage, please contact us here *(Note: Please ensure you select the correct location / country of your residence by clicking the button in the top left corner).*

You will still see "contextual" ads even if you opt out of interest-based ads. Even if we stop sending you interest-based ads, you will still get ads from our brands on your computer or mobile devices. These ads, however, are based on the context of the sites you visit and are called contextual ads. Unlike interest-based ads which are based on pages you visit on your mobile phone or computer viewing activities over time and across unrelated services, contextual ads are ads shown to you based on the context of the specific site you are visiting. For example, you still may see an ad for one of our baby care brands while looking at nursery products online because these sites traditionally have had mostly new or expecting parents as visitors. You should also know that we may still collect information from your computer or devices and use it for other purposes like evaluating how our websites work, for consumer research, or detecting fraud, pursuant to applicable laws.

How You Can Control Cookies

You can set your browser to refuse all cookies or to indicate when a cookie is being sent to your computer. However, this may prevent our sites or services from working properly. You can also set your browser to delete cookies every time you finish browsing.

When you opt-out of interest-based advertising, an opt-out cookie is sent to your browser that indicates that you no longer want to receive interest-based ads. Your opt-out cookie will be deleted if you decide to delete all cookies on your browser. This means that you will need to opt-out again on each browser where you have deleted cookies if you still do not want to receive interest-based ads.

In some markets and on some of our websites, we offer a cookie consent management platform which allows you to exercise choice with respect to certain categories of cookies. If this is available, this may appear as a cookie banner and/or as an icon that is visible on the applicable websites. We may also provide similar technology in mobile apps, which, if available, will be accessible through the applicable app's settings menu.

U.S. State Privacy Laws

See our "U.S. State Privacy Notice " below for information required by certain state privacy laws, and information regarding privacy rights under such laws.

Additional Information for EEA, Switzerland, UK and Serbia Residents

If you live in the EEA, Switzerland, the UK or Serbia, or are physically in the EEA, Switzerland, Serbia or the UK, you may access the personal data we hold about you, request that inaccurate, outdated, or no longer necessary information be corrected, erased, or restricted, and ask us to provide your data in a format that allows you to transfer it to another service provider. You also may withdraw your consent at any time where we are relying on your consent for the processing of your personal data. And you may object to our processing of your personal data (this means ask us to stop using it) where that processing is based on our legitimate interest (this means we have a legitimate reason for using the data for a certain purpose and this reason is not outweighed by your interest in P&G not using it). To make a request, please contact us.

If you would like more information about data protection and your personal data rights in general, please visit the European Data Protection Supervisor's site at https://edps.europa.eu/data-protection/ or the UK Information Commissioner's Office site at https://ico.org.uk or the or the Swiss Federal Data Protection and Information Commissioner site at https://www.edoeb.admin.ch/edoeb/en/home.html the Serbia Commissioner (for information of public importance and personal data protection of personal data) at https://www.poverenik.rs/en/home.html. If you are not happy with our response to your requests, you may lodge a complaint with the data protection authority in your country.

Procter and Gamble España SA adheres to the Code of Conduct for Data Protection in AUTOCONTROL, accredited by the Spanish Data Protection Agency and therefore is subject to its extrajudicial system of data processing complaints when related to data protection and advertising, available for those interested on the website www.autocontrol.es.

Dental Professionals

If you are a dental professional and have provided your personal data to us as part of one of our professional outreach programs, including through https://www.dentalcare.com, please contact us through your local P&G representative, e.g. Oral-B.

Healthcare Professionals

If you are a healthcare professional and have provided your personal data to us as part of one of our professional outreach programs or any other form of collaboration, please contact us through your local or regional P&G representative.

Consumer Research Participants

To make a request with respect to personal data we may have as part of your participation in one of our research studies, please see the contact information provided on your consent form or call or visit your research center.

How We Gather & Use Personal Data

Like most brands, we collect personal data as you interact with us or when you share personal data with third parties that in turn can be shared with us. We do this respectfully and carefully to protect your rights. Personal data can help us better understand your interests and preferences as a consumer and a person.

How We Collect Personal Data

We collect personal data about you in many ways and from many places. Some of the personal data we collect may include personal data that can be used to identify you; for example, your name, email address, telephone number, or postal address. In some jurisdictions, things like IP address or cookie and mobile device identifiers may also be considered personal data. Some of the personal data we collect may be considered sensitive personal data or special category data and may include, account login information, financial information, precise geolocation data, government identifiers, racial or ethnic origin, mental & physical health / condition, Consumer Health Data, sex

life or sexual orientation, transgender / non binary status, children's data, criminal background, genetic data and biometric data for the purpose of uniquely identifying an individual etc.

You Share it Directly

You give us your personal data directly for example when signing up for an account on our websites or mobile apps or by calling or emailing us, or while participating in a P&G survey or contest etc. We may ask for things like your name, email or home address, date of birth, payment information, your age, gender, the number of people in your family, and the way you want us to send you information about our products and services—for example, to your home address, email address, or by texting you.

You Interact with Websites & Emails

We may use technologies that automatically collect information when you visit our sites, view our advertisements, or use our products or services. For example, we use cookies (a tiny file stored on your computer's browser) to tell us what browser and operating system you are using, your IP address, and about your online activities such as web pages you visit, links you click, or whether you have or have not opened an email from us.

You Use Mobile Apps & Other Devices

To give you the best possible user experience, we may use technologies that collect information from your phone when you use our mobile apps or our "smart" devices in your home. You consent to this when downloading the app or installing household internet connected devices. This information could include your mobile phone or other device advertising ID, information about your phone's operating system, how you use the app or device, your physical location, and other information that is considered personal data in some jurisdictions. You will get a pop-up notice on your phone or device that gives you the option to accept or reject allowing us to know your precise geolocation (exactly where you are standing or where you are accessing the internet) or to collect or access other personal data, as required by the applicable laws.

You Connect with Partners or Third Parties

We may get information that other companies share with or sell to us. For example, you may have given consent for another company to share your personal data with us when you signed up for telecom services or a retailer loyalty points program. Where possible, we may also collect personal data from publicly available sources, such as from internet postings, blog entries, videos, or social media sites. We may also receive

personal data from other companies, such as consumer data resellers, who are in the business of collecting or aggregating information about you sourced from publicly available databases (in line with local legal requirements as applicable) or from consent you have given to their use and subsequently our use of your personal data. This might include information about your income level, age, gender, number of people in your family, and products you have bought on the internet or from stores in your neighborhood.

General Ways We Use Personal Data

We use your personal data to help us meet our purpose of touching and improving the lives of people like you every day around the world. For example, we use your information for the following Processing Purposes:

- Products/Services. This includes performing services for you and sending you products or samples you have requested.
- Customer Management. This includes:
  - Identifying and authenticating you to our different marketing programs and websites
  - Administering and maintaining accounts and preferences, as well as financial incentive, rewards, discounts (e.g., price or service coupons) and loyalty programs (collectively, “Rewards Programs”)
  - Helping you manage your P&G site or app preferences
  - Allowing you to enter our contests or sweepstakes and leaving ratings and reviews
- Customer Service/Communications, such as:
  - Responding to your questions or requests for information
  - Providing customer service
  - Sending transactional messages (such as account statements or confirmations)
  - Interacting with you on social media
  - Sending marketing communications about our products or services (or the products or services of our partners), survey, and invitations
- Payment/Financial, such as:

- Processing your payment for the products you buy from us
- Processing and issuing refunds and collections

- Serving Ads. This includes serving you with relevant ads and serving others, who, having a profile like yours, may be interested in hearing from us, with relevant ads through custom audiences and look-alike audiences. For example, we may upload your hashed email address into a social media service and ask that social media service to send our ads to you and to people who have similar interests as you, including in other countries, based on data it has about you and about other people
- Ads Administration, such as measuring and tracking the effectiveness of advertising campaigns and carry out other administrative and accounting activities with respect to ad campaigns
- Quality and Safety, including:
  - Quality control, training, and analytics
  - Safety maintenance and verification
  - System administration and technology management, including optimizing our websites and applications
- Security, including detecting threats and protecting against malicious or fraudulent activity
- Recordkeeping and Auditing, including recordkeeping and auditing interactions with consumers, including logs and records maintained as part of transaction information
- Legal/Compliance, including risk management, audit, investigations, reporting and other legal and compliance reasons.
- Research & Development ("R&D"), such as
  - Internal research
  - To design and develop products, services and programs that delight our consumers
- **Purposes Disclosed at Collection** when you provide your personal data
- **Legitimate Business Purposes** that are compatible with the purpose of collecting

your personal data and that are not prohibited by law

How We Use Cookies

Cookies are small files sent to your computer as you surf the web. They store useful information about how you interact with the websites you visit. You can learn more about how to control cookies here.

We use cookies in several ways, such as:

- to allow you to browse the website and use its features
- to serve you with relevant advertising and measure the effectiveness of such advertising
- to ensure that you are not shown an ad more than you should be (called “frequency capping”)
- to learn more about the way you interact with P&G content
- to help us improve your experience when visiting our websites
- to remember your preferences, such as a language or a region, so there is no need for you to customize the website on each visit
- to identify errors and resolve them
- to analyze how well our websites are performing

Types of Cookies We Use

Strictly Necessary Cookies: These cookies (also sometimes referred to as “essential”) allow the page to load or provide some essential functionality without which the page would not work (i.e., store your data in a shopping cart).

Functional Cookies: These cookies allow sites to remember what you prefer when you come back again. For example, if you choose to read the site in French on your first visit, the next time you come back the site will appear automatically in French. Not having to select a language preference every time makes it more convenient, more efficient, and user-friendly for you.

Advertising / Targeting Cookies: These cookies can be used to learn about what interests you generally might have, based, for example, on the websites you visit and the products you buy. That data allows us to send you ads for products and services

that better fit the things you like or need. It also allows us to limit the number of times you see the same advertisement.

Analytics / Performance Cookies: These cookies tell us how you use our websites, like which pages you visited and which links you clicked. This helps us measure and improve the performance of our websites. We use different analytics cookies in different jurisdictions. In many cases, we use Google Analytics cookies to monitor the performance of our sites. Our ability to use and share information collected by Google Analytics about your visits to our sites is restricted by the Google Analytics Terms of Use and the Google Privacy Policy.

Social Media Cookies: These cookies, that are set by a range of social media services that we have added to the site, allow you to share our content with your friends and networks and enable us to reach you with ads on those social platforms related to your visits on our sites. The cookies of some social media sites, e.g., Facebook, are also used for ad targeting.

Interest-Based Advertising

When you visit our partner sites, we can show you ads or other content we believe you would like to see. For example, you may receive advertisements for Tide® laundry detergent if we notice that you are visiting sites that sell children's clothing or school supplies. And from that information we may conclude that you have children and therefore could well be interested in a powerful laundry-cleaning product. In this way, we intend to send you relevant information about our products that might be of benefit to you. To learn more about your choices regarding interest-based advertising go here.

We Learn from Groups of Consumers Sharing Similar Interests: We may place you into a particular group of consumers who show the same interests. For example, we may put you in the group of "razor aficionados" if we see you frequently purchase razors online or you could be a "bargain-shopper" if we notice you use online coupons or look for discounts or sales. We may infer these things about you based on your activity on certain web pages, links you click on our websites and other websites you visit, mobile applications you use, or our brand emails you view and links you click in the emails, as well based on other information we have collected, such as from retailer partners and other third parties. We group together cookie and device IDs to help us learn about general trends, habits, or characteristics from a group of consumers who all act similarly online and/or offline. By doing this, we can find and serve many others who "look like" those already in the group and thereby send them what we believe will be relevant and beneficial product offers and information.

We Link Other Information to Your Cookie and Device IDs: Your cookie and device IDs may be supplemented with other information, such as information about the products you buy offline or information that you provide directly to us when creating an account on our sites. We generally do this in ways that will not directly personally identify you. For example, we could know that cookie ID ABC12345 belongs to the razor aficionado group based on a person's web site visits, age, gender, and shopping habits. Should we want to personally identify your cookie or device information (web and app viewing history), we will do so in accordance with applicable laws.

We May Know You Across Your Computers, Tablets, Phones and Devices: We may know that cookie ID ABC12345 is from a computer that that may be connected to the same person or household owning the mobile phone with device ID EFG15647. This means that you may search for diapers on your laptop, click on a Google search result link which we have sponsored, and then later see an ad for our Pampers® brand diapers on your mobile phone. We might assume or deduce that the same person owns the computer and phone because, for example, they sign on to the same Wi-Fi network every day at the same time. Understanding what devices seem to be used by a person or household helps us limit the number of times you see the same ad across your devices. And this is important because that way you don't get annoyed at us for spamming you with the same ad and we don't pay for such repetitive ads that we don't want you to receive.

Addressable Media: When you provide us with your personal data via our sites or apps, we may use an encryption of that data – or a substitute identifier such as The Trade Desk's UID2 -- to serve you with ads we think you may like. We do this generally by uploading a pseudonymized version (replaced with artificial letters or numbers) of your email address, phone number, or your mobile advertising ID to a platform that offers ad space (e.g., Facebook, YouTube, Instagram, TikTok, etc.). We also use that same data to serve you advertising through what is called the open web. This means you may see relevant ads from us on sites like nytimes.com or apps or other places like digital TV that participate in online auctions of their ad inventory.

Advanced Matching: Some of our sites use the Advanced Matching features offered by Social Media Platforms to its advertisers (e.g. Facebook's Advanced Matching, TikTok's Advanced Matching, etc.). Through Advanced Matching, we may send some of the personal data you enter on our site form fields (e.g., your name, email address, and phone number – not any sensitive personal data or special category data) in a pseudonymized format to the Social Media Platform, or the Social Media Platform Pixel will pseudonymize and pull that data automatically, for the purpose of helping associate you with your browser cookie or device ID. We do this so that we can better target and measure the effectiveness of our advertising on the respective Social Media platforms. This is how we can know that if we showed you an ad on a given Social Media Platform, you clicked on it, came to our site and bought something – or not –

and therefore whether we should continue to buy ads on that Social Media Platform – or not.

Google Analytics Advertising Features: Some of our sites use Google Remarketing Lists for Search Ads with Analytics ("RLSA"), which is a service they offer to advertisers. When individuals visit our sites, Google Analytics collects data about their visits (and not any sensitive personal data or special category data). If a visitor is signed into their Google account, we are able to provide that user with interest-based advertising when they conduct a Google search for terms related to the P&G site they visited. For example, if you are signed into a Google account when visiting our Head & Shoulders website, we may provide you with Head & Shoulders advertising when you search for "dandruff shampoo" on Google. Our ability to use and share information collected by Google Analytics about your visits to our sites is restricted by the Google Analytics Terms of Use and the Google Privacy Policy. To understand how Google uses data when you use our partners' sites or apps, visit here. You may opt out of Google Analytics at any time.

Other Technologies We May Use

Proximity-Based Beacons: Beacons send one-way signals to mobile apps you install on your phone over very short distances to tell you, for example, what products are on-sale as you walk through a store. Beacons only talk to your device when you get close enough and after you have given consent within the mobile application associated with a particular beacon. In turn, apps may provide us location information to help customize advertising and offers to you. For example, when you are near a beacon in the skin care section of a supermarket, we may send you a $4 off coupon.

Pixels: These are small objects embedded into a web page but are not visible. They are also known as "tags," "web bugs," or "pixel gifs." We may use pixels to deliver cookies to your computer, monitor our website activity, make logging into our sites easier, and for online marketing activities. We may also include pixels in our promotional email messages or newsletters to determine whether you open them and click on their links. This helps us understand whether you are an active user (which will prevent your data from being deleted due to inactivity). It also helps us measure the effectiveness of our marketing efforts, and derive insights and analysis, that we will use to personalize the content of our communication and to guide our marketing decisions (for example, if you opened an email but did not click on the links in it, we may decide to retarget you on Facebook).

Mobile Device Identifiers and SDKs: We use software code in our mobile apps to collect information as you use our apps which is like what cookies collect on our websites. This will be information like your mobile phone identifiers (iOS IDFAs and Android Advertising IDs) and the way you use our apps.

Precise Geolocation: We may receive information about your exact location from things like global positioning system (GPS) coordinates (longitude and latitude) when you use our mobile apps. You will always get a pop-up notice on your phone or device asking for you to accept or reject allowing us to know exactly where you are in the world. You should understand that we will not always ask for consent to know generally that you are in a broader city, postal code, or province. For example, we do not consider it to be precise location if all we know is that you are somewhere in Manila, Philippines.

Site and App Content

Plugins: Our websites may include plugins from other companies such as social networks. An example of a plugin is the Facebook "Like" button. These plugins may collect information (e.g., the URL of the page you visited) and send it back to the company that created them. This may happen even if you do not click on the plugin. These plugins are governed by the privacy policy and terms of the company that created them, even though they appear on our sites.

Logins: Our websites may allow you to log in using your account with another company such as, for example, "Login with Facebook." When you do this, we will have access only to the information that you have given us consent to receive from your account settings in the other company's account you're using to log in with.

User Content: Some of our sites and apps will allow you to upload your own content for contests, blogs, videos, and other functions. Please remember that any information you submit or post becomes public information. We do not have control over how others may use the content you submit to our sites and apps. We are not responsible for such uses in ways that may violate this privacy policy, the law, or your personal privacy and safety.

Links: P&G sites may include links to other sites, which we do not control. Those sites will be governed by their own privacy policies and terms, not ours.

Automated Decision-Making and Profiling

Automated decision-making implies making a decision using automated means without human involvement. Profiling is a form of automated processing of personal data consisting of the use of personal data to evaluate certain personal characteristics of an individual for the purpose of analyzing or predicting, for example, that individual's personal preferences, interests, likely behavior, etc.

As you have read in this Privacy Policy, we collect a variety of types of personal data both from you and from other commercially available sources. This data may be

combined and analyzed, including sometimes using algorithms, to identify links between certain behaviors and personal characteristics. P&G users who have similar characteristics or have performed similar actions are likely to share similar interests in our products: based on this analysis, segments of P&G consumers are created and targeted accordingly with relevant offers via email, online advertising, and social media.

This process allows us to customize our communications to your declared or inferred interests. However, we will not conduct any automated decision-making processes, including profiling, that can produce legal effects or that can similarly significantly affect your rights and freedoms, as per Art. 22(1) and (4) of the GDPR and, should we want to engage in more intrusive profiling and tracking practices, we will always inform you and, where legally required, ask for your consent before doing so or provide you with the right to opt-out.

How We Disclose Personal Data

With Your Consent

When we have your consent, we may disclose your personal data to others, such as select partners so they can send you offers, promotions, or ads about products or services we believe you may be interested in. For example, people who receive P&G emails from our diaper brands such as Pampers® may also consent to hear about baby formulas from other companies.

Online Platforms and Ad Tech Companies

Our websites and applications may make available contact information, unique identifiers, inferred and derived information, online and technical information and geolocation data with online platforms and ad tech companies to help us serve you relevant advertisements and offers, subject to applicable legal requirements, which may include consent and/or opt-outs. We do not sell your personal data to marketers outside of P&G in exchange for monetary compensation. Please see the U.S. State Privacy Notice section of the privacy policy below for additional information.

Vendors

We may disclose or otherwise make available your personal data to our vendors (including “service providers” and “processors” defined under applicable laws, which we collectively refer to as “**service providers**” or “**vendors**” herein) who help us run our business. This includes hosting our sites, processing payment information for the purchases made by you through our sites, delivering our emails and marketing

communications to you, analyzing the data we collect, helping us with sales attribution (e.g., to see if we showed you an ad on a platform site and then you bought a product from us) and sending you the products and services you requested. We also disclose or otherwise make available your personal data with lawyers, auditors, consultants, information technology and security firms, and others who provide services to us. We disclose or otherwise make available only the personal data needed for these companies to complete the tasks we request or, where permitted by applicable law, use the personal data for certain internal purposes such as security or fraud detection. We instruct our service providers to appropriately process and protect your personal data.

Payments for Purchases

Payments for purchases made through some of our sites are completed using a third-party vendor's online payment system. For these sites, P&G does not have access to your credit card information provided for purchases and does not store or disclose your credit card information as part of your purchases through these third-party systems. The personal or financial information you provide to our online payment system on these sites is subject to the third-party's privacy policy and terms of use and we recommend you review these policies before providing any personal or financial information.

Legal and Similar Reasons

If a brand or one of our businesses that controls your personal data, or some or all of its business assets, are sold to another company, your personal data will be disclosed to that company. We may also disclose your information to companies who help us protect our rights and property, or when required by law, legal processes, government authorities or as reasonably necessary to protect the rights or interests of ourselves or others.

Types of Personal Data We Collect

As a large company, with many products and businesses in many countries around the world, we collect the following types of personal data to best serve our consumers.

Please be aware that this is a comprehensive list of various types of personal data we collect and that we only collect it in accordance with legal requirements and when have a lawful basis to do so (for example when we have your consent, or when we need this information for the performance of a contract to which you are party, or when the processing is necessary based on our legitimate interest or for compliance with a legal obligation). Many of these data collection types almost certainly will not apply to you. If you want to know what

data we actually have about you, please contact us here *(Note: Please ensure you select the correct location / country of your residence by clicking the button in the top left corner)*.

What We Typically Collect

Contact Information: Data elements in this category include names (including nicknames and previous names), titles, mailing address, email address, telephone/mobile number and contact information for related persons (such as authorized users of your account).

General Demographics & Psychographics: Data elements in this category include personal characteristics and preferences, such as age range, marital and family status, race and ethnicity (for example, in relation to information you provide in relation to your haircare or skincare purchases or preferences), 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: Data elements in this category include customer account information, qualification data, purchase history and related records (returns, product service records, records of payments, credits etc.), 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 & Accounts Details: Data elements in this category include unique ID number (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: This includes internet or other electronic network activity information. Data elements in this category include IP addresses, MAC addresses, SSIDs or other device identifiers or persistent identifiers, online user IDs, encrypted passwords, 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, web beacons, clear gifs and pixel tags. This also includes information such as your device functionality (browser, operating system, hardware, mobile network information); the URL that referred you to our website; the areas within our website or apps that you visit and your activities there (including emails, such as whether you open them or click on links within); your device characteristics; and device data and the time of day.

Inferred Information: This includes information derived from other personal data listed in this section. We create inferred and derived data elements by analyzing all personal data we may have about you. Data elements in this category include propensities, attributes and/or scores generated by internal analytics programs.

What We Sometimes Collect

What We Sometimes Collect – Sometimes we collect sensitive personal data or special category data and we do it only in accordance with the legal requirements and when we have a lawful basis to do so (for example when we have your consent, or when we need this information for the performance of a contract to which you are party, or when the processing is necessary based on our legitimate interest or for compliance with a legal obligation).

Precise Geolocation: Data elements in this category include precise location (such as latitude/longitude).

Health-Related Information: Data elements based on how it is collected include:

- Information collected from consumer programs (such as when you register on our brand sites, participate in our rewards programs, or purchase our products)
    - General health and symptom information, such as dandruff & hair loss, diaper rash etc.
    - Pregnancy-related information, such as due date
- Consumer Research Studies where you have provided your informed consent
    - Information about physical or mental health, disease state, medical history or medical treatment or diagnosis, medicines taken and related information
- Information collected when you contact us to report a complaint or an adverse event occurring in connection with the use of one of our products

Financial Account Information: Data elements in this category include bank account number and details and payment card information (e.g., when you make a purchase directly with a brand or receive a credit from a brand).

Government-Issued IDs: Data elements in this category include governmental ID and Tax ID (e.g., for winners of a contest in jurisdictions where we are required to collect that information).

Audio Visual Information: Data elements in this category include photographs, video images, CCTV recordings, Call Center recordings and call monitoring records and voicemails (e.g., for research, when you visit our facilities, or when you call us).

Smart Devices and Sensor Information: Data elements in this category include smart device records, IoT products (e.g., from an Oral B app-connected toothbrush).

Data About Children: Data elements in this category may include the number of children you have, your children's diaper sizes, their genders, and ages.

Biometric Information: Data elements in this category include facial recognition data, and a mathematical representation of your biometric identifier, such as the template maintained for comparison (e.g., for healthcare research studies).

Legal Basis & Retention by Processing Purpose

Generally, we keep your personal data for only as long as it is needed to complete the processing purpose for which it was collected or as required by law. We may need to keep your personal data for longer than our specified retention periods to honor your requests, including to continue keeping you opted out of marketing emails, or to comply with legal or other obligations. This section outlines why the processing purposes comply with the law (legal basis, as required by certain non-U.S. Privacy Laws such as the GDPR), and how long we keep the personal data used for that processing purpose, unless an exception applies (retention period), such as the ones noted above. Some U.S. Privacy Laws (defined below) require us to, on a per-category basis, disclose the retention period applicable to each such category of personal data. See the table set forth in our U.S. State Privacy Notice for this information.

Products/Services

Legal Basis:

- Performance of a Contract for fulfilling eCommerce sales
- Consent for sampling programs
- Legitimate Interest or consent for coupon issuing and coupon clearing

Retention Period: After no longer needed to provide you with the requested products or services unless required by law or contract to retain it further.

Customer Management

Legal Basis:

Consent for:

- sending you (personalized) marketing email and text communications
- processing your ratings and reviews of our products
- collection and analysis of the information contained on the purchase receipts you upload for more personalized advertising
- adverse event reporting
- the processing of certain sensitive personal data or special category data
- non-essential tracking technologies on our websites and in our mobile apps in certain countries

Legitimate Interest for:

- consumer complaint handling & complaint investigation (unless consent is required according to country laws).
- postal marketing (unless consent is required according to country laws)
- delivering requested items to you
- processing your personal data within our various marketing systems

Depending on the case, we may rely on our Legitimate Interest or Consent for:

- the enrichment and combination of your registration data (including data that you disclose to us when interacting with our services, such as brand preferences, clipped coupons, etc.) with attributes, interests or demographic data obtained from commercially available sources or other third parties
- delivering personalized ads to you and individuals with similar profiles across online channels.

Performance of a Contract for:

- contests, cash back and loyalty rewards membership (unless consent is required according to country laws) managing warranty claims

Retention Period: Until you request to delete the personal data or withdraw your consent. Otherwise, we will delete your personal data after no longer needed for the processing purpose or after a maximum of 50 months of non-activity unless required by law or contract to retain it further. We define inactivity through several internal criteria that indicate a user's lack of interaction with our programs and communications. For example, if you do not log in, or do not open or click on our emails, we will consider you "inactive" and delete your data after a maximum of 50 months but sooner for certain countries depending on local legal requirements. We may need to keep some of your personal data to honor your requests, including to continue keeping you opted out of marketing emails, or to comply with other legal obligations. We may also retain certain personal data used in ratings and reviews for as long as the review is used or until the product is discontinued.

Customer Service/Communications

Legal Basis:

Legitimate Interest for:

- managing consumer and business inquiries

Consent for:

- sensitive personal data or special category data which may be collected in some adverse event cases

Performance of a Contract for:

- sending transactional/program information about your accounts, purchases, reward terms, etc.
- engagement with professional influencers, business contacts, ambassadors, etc.

Retention Period: Until you request to delete the personal data or withdraw your consent. Otherwise, we will delete your personal data after no longer needed for the processing purpose unless required by law or contract to retain it further.

Payment/Financial

Legal Basis: Performance of a Contract

Retention Period: As long as necessary to fulfill the order unless required by law or contract to retain it further. We generally retain data for 24 months for cashback offers

and 10 years for warranties.

Serving Ads

Legal Basis:

- When we deploy tracking technologies on our own websites or within our own mobile applications, we comply with the legal requirements and we rely on consent or legitimate interest, as required by the laws of the country. Even when we place tracking technologies on third-party properties or buy data from third-party vendors, we require them to comply with the legal requirements (including obtaining your consent before deploying our tracking technology or sharing your personal data with us if needed).

- Legitimate Interest or consent depending upon the legal requirement, for processing your email address, phone number, or mobile advertising ID to serve you relevant advertising across different media channels, including on social media platforms, via custom audiences and look-a-like audiences.

Retention Period: After no longer needed for the processing purpose (i.e., after the ad campaign ends) or within a maximum of 110 months unless you opt-out sooner.

Ads Administration

Legal Basis: Legitimate Interest

Retention Period: After no longer needed to fulfill the processing purpose. For personal data collecting via tracking technologies on our websites or within our mobile applications, within 12 months unless you opt-out prior

Quality & Safety

Legal Basis: Legitimate Interest

Retention Period: After no longer needed to fulfill the processing purpose unless required by law or contract to retain it further. For personal data collecting via various tracking technologies on our websites or within our mobile applications, within 12 months unless you opt-out prior.

Security

Legal Basis: Legitimate Interest

Retention Period: After no longer needed to fulfill the processing purpose unless required by law or contract to retain it further. For personal data collecting via tracking technologies on our websites or within our mobile applications, within 12 months.

Recordkeeping and Auditing

Legal Basis:

- Performance of a Contract for transactional data
- Legal Obligation for certain recordkeeping activities

Retention Period: After no longer needed to fulfill the processing purpose unless required by law to retain it further.

Legal/Compliance

Legal Basis: Legal Obligation

Retention Period: After no longer needed to fulfill the processing purpose unless required by law to retain it further.

Research & Development ("R&D")

Legal Basis: Consent

Retention Period: We retain non-biometric personal data collected from clinical research as long as needed for the purpose for which it was collected, or 30 years after the purpose of collection is fulfilled, and/or for as long as may be required to retain it by local law, regulation or good clinical research practice, whichever is later. For non-clinical research, we will retain non-biometric personal data for a maximum of 5 years after the time of collection, or after the purpose of collection is fulfilled, whichever is later. For biometric data, we will retain for as long as necessary to fulfil the purpose of collection or processing, unless we are required to retain it longer for legal or regulatory compliance purposes, or to exercise or defend our legal interests. We may retain your signed informed consent documents longer.

Children's Personal Data

We only collect children's data in limited circumstances and always in accordance with applicable data protection laws. We do not use personal data collected from children for

targeted advertising.

How We Protect Your Personal Information

Your privacy is important. That's why we respect it by taking steps to protect your personal data from loss, misuse, or alteration.

We have processes and controls in place to appropriately manage personal data, including its collection, use, disclosure, retention, and destruction. We respect your personal data and take steps to protect it from loss, misuse, or alteration. Where appropriate, these steps can include technical measures like firewalls, intrusion detection and prevention systems, unique and complex passwords, and encryption. We also use organizational and physical measures such as training staff on data processing obligations, identification of data incidents and risks, restricting staff access to your personal information, and ensuring physical security including appropriately securing documents when not being used.

International Transfers

P&G has its head offices in the United States, regional offices in Singapore, Dubai, Geneva and Panama and further P&G service centers in other countries, like Costa Rica or Philippines. As a multinational company, P&G undertakes data transfers, either within the P&G group of entities, or when sharing your data with service providers or selected partners that may store, process, or access your data in a country other than the one in which it was collected, including the United States. Personal data collected from Quebec, for example, may be transferred outside of Canada with adequate protections and safeguards in place.

As far as EU citizens are concerned, (but also citizens of Switzerland, UK and Serbia for example) this means that their data may be processed outside of the European Economic Area (EEA), either in countries that have been recognized by the European Commission to offer adequate data protection, like the United Kingdom (from where, for example, some of our fulfillment, return and contact center services are managed for the EU region), or Switzerland (where our EU headquarters are located), or in other countries that are not deemed, by the European Commission, as offering such level of data protection. For such transfers of data, because special safeguards need to be foreseen to ensure that the protection travels with the data, we use the EU Standard Contractual Clauses, standardized and pre-approved model data protection clauses. You can find the latest version of the approved EU Standard Contractual Clauses, including the different transfer modules, here. Our transfer agreements also incorporate the standard data protection clauses issued in accordance with UK, Swiss and Serbian data protection law If you have any questions with reference to our data transfer agreements, please contact us.

If you are located in the European Economic Area (EEA), United Kingdom (and Gibraltar) or Switzerland, please note that P&G is certified under 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 "Data Privacy Framework"] developed by the U.S. Department of Commerce and the European Commission and Information Commissioner and Swiss Federal Data Protection, respectively, regarding the transfer of personal information from the EEA, United Kingdom (and Gibraltar) or Switzerland to the U.S., Click here to view our *Data Privacy Framework: Consumer Privacy Policy*.

For non-EEA and UK data, we perform such transfers based on your consent, or on our contracts, where so required by local law.

Additional Regional Notices

U.S. State Privacy Disclosure and Consumer Rights ("U.S. State Privacy Notice")

This U.S. State Privacy Notice applies to "Consumers" as defined under U.S. privacy laws, specifically the California Consumer Privacy Act, including as amended by the California Privacy Rights Act ("**CCPA**"), the Virginia Consumer Data Privacy Act ("**VCDPA**"),the Colorado Privacy Act, the Utah Consumer Privacy Act, Connecticut's Act Concerning Personal Data Privacy and Online Monitoring, and any other U.S. privacy laws, as each are amended and as and when they become effective, and including any regulations thereunder (collectively, the "**U.S. Privacy Laws**"). This U.S. State Privacy Notice is a supplement to this Privacy Policy. In the event of a conflict between any other P&G policy, statement, or notice and this U.S. State Privacy Notice, this U.S. State Privacy Notice will prevail as to Consumers and their rights under the applicable U.S. Privacy Laws.

This U.S. State Privacy Notice is designed to provide you with notice of our recent personal data practices over the prior 12 months from the "Last Updated" date of this Privacy Policy. This U.S. State Privacy Notice will be updated at least annually. ***This U.S. State Privacy Notice also applies to our current data practices such that it is also meant to provide you with "notice at collection,"*** which is notice of personal data (also referred to in some of the U.S. Privacy Laws as "personal information") we collect online and offline, and the purposes for which we process personal data, among other things required by the U.S. Privacy Laws. For any new or substantially different processing activities that are not described in this U.S. State Privacy Notice, we will notify you as required by the U.S. Privacy Laws, including by either notifying you at the time of collecting personal data, or by updating this U.S. State Privacy Notice earlier than required. We reserve the right to amend this U.S. State Privacy Notice at our discretion and at any time. To contact us about this U.S. Privacy Notice, please see the Contact Us section below.

Generally, we collect, retain, use, and disclose your personal data for our business purposes and commercial purposes, which are described above in the remainder of this Privacy Policy, including in "How We Gather & Use Personal Data,"and "How We Disclose Personal Data" (collectively, our "**Processing Purposes**"). The sources from which we collect personal data are set forth above in the "How We Gather & Use Personal Data." Some of the Processing Purposes, as we discuss below in the table, implicate "Sale," "Sharing", and or "Targeted Advertising." For more details on the meaning of Sale, Sharing, and Targeted Advertising, see the "Do Not Sell/Share/Target" section below. Please note that the Processing Purposes as shown in the table are categorical descriptions, to aid in readability and clarity. Please reference the "General Ways We Use Personal Data" section of the Privacy Policy above for the full description of each Processing Purpose.

The table below describes the categories of personal data we collect in the first column (starting on the left). The second column provides examples of data types within the applicable categories, which, in some instances, include the personal data types/categories listed above under "Types of Personal Data We Collect." The third column states the categories of recipients that receive such personal data (including sensitive personal data or special category data) as part of disclosures for business purposes, as well as disclosures which may be considered a Sale or Share under certain U.S. Privacy Laws. Not all data indicated in the examples is "sold" to third parties. For example, in the "Identifiers and Contact Information" of the chart, we may collect "financial account data" or "government issues IDs" in order to provide services to you, but we do not "sell" it to third parties. However, we may sell "unique IDs" and account information to third parties. If any of your data is "sold" or "shared," it will be done so according to applicable law. The fourth column provides the Processing Purposes that are applicable to each category of personal data. In the fifth column, we provide, on a per category of personal data basis, the applicable retention period.

Category of Personal Data	**Examples of Personal Data Types within Category**	**Categories of Recipients**	**Processing Purposes**	**Retention Period**
1. Identifiers and Contact Information	Contact information, Unique IDs & Accounts Details, Online and Technical Information, Financial Account Information, Government-issued IDs	Disclosures for Business Purposes: • Software and other business Vendors ("Business Vendors") • Marketing Vendors • Affiliates and Related Entities	• Products/Services • Customer Management • Customer Service/Communications • Payment/Financial • Serving Ads • Ads Administration • Quality and Safety • Security • Recordkeeping • Legal/Compliance • R&D • Purposes Disclosed at Collection	After no longer needed for the processing purpose(s) or after a maximum of 50 months of non-activity unless required by law or contract to retain. Data necessary to suppress communications to opted out

		Sale/Sharing: Third-Party Digital Businesses and Retail Partners	• Legitimate Business Purposes	consumers may be retained further.
2. Personal Records	Contact information, Unique IDs & Accounts Details, Financial Account Information, Government-issued IDs	Disclosures for Business Purposes: • Business Vendors • Marketing Vendors • Affiliates and Related Entities Sale/Sharing: Third-Party Digital Businesses	• Products / Services • Customer Management • Customer service / communications • Payment / financial • Serving ads • Ads Administration • Quality and Safety • Security • Recordkeeping • Legal / Compliance • R&D • Purposes Disclosed at Collection • Legitimate Business Purposes	After no longer needed for the processing purpose(s) or after a maximum of 50 months of non-activity unless required by law or contract to retain. Data necessary to suppress communications to opted out consumers may be retained further.
3. Personal Characteristics or Traits	General Demographics & Psychographics, Data About Children, Inferred Information, Health-related information	Disclosures for Business Purposes: • Business Vendors • Marketing Vendors • Affiliates and Related Entities Sale/Sharing: Third-Party Digital Businesses and Retail Partners	• Products / Services • Customer Management • Customer service / communications • Payment / financial • Serving ads • Ads Administration • Quality and Safety • Security • Recordkeeping • Legal/Compliance • R&D • Purposes Disclosed at Collection • Legitimate Business Purposes	After no longer needed for the processing purpose(s) or after a maximum of 50 months of non-activity.
4. Customer Account Details / Commercial Information	General Demographics & Psychographics, Transaction and Commercial Information, Online & Technical Information	Disclosures for Business Purposes: • Business Vendors • Marketing Vendors • Affiliates and Related Entities Sale/Sharing: Third-Party Digital Businesses	• Products/Services • Customer Management • Customer Service/Communications • Payment/Financial • Serving Ads • Ads Administration • Quality and Safety • Security • Recordkeeping • Legal/Compliance • R&D • Purposes Disclosed at Collection	After no longer needed for the processing purpose(s) or after a maximum of 50 months of non-activity.

		and Retail Partners	• Legitimate Business Purposes	
5. Biometric Information	Biometric Information	Disclosures for Business Purposes: • Business Vendors • Affiliates and Related Entities Sale/Sharing: N/A	• Products/Services • Customer Management • Customer Service/Communications • Quality and Safety • Security • Recordkeeping • Legal/Compliance • R&D • Purposes Disclosed at Collection • Legitimate Business Purposes	After no longer needed for the processing purpose(s) unless required to retain for legal or regulatory compliance.
6. Internet/App Usage Information	Transaction and Commercial Information, Online & Technical Information, Smart Devices and Sensor Data	Disclosures for Business Purposes: • Business Vendors • Marketing Vendors • Affiliates and Related Entities Sale/Sharing: Third-Party Digital Businesses	• Products/Services • Customer Management • Customer Service/Communications • Payment/Financial • Serving Ads • Ads Administration • Quality and Safety • Security • Recordkeeping • Legal/Compliance • R&D • Purposes Disclosed at Collection • Legitimate Business Purposes	After no longer needed for the processing purpose(s) or after a maximum of 50 months of non-activity unless required by law or contract to retain.
7. Location Data	Imprecise Location Data, Precise Geolocation Data	Disclosures for Business Purposes: • Business Vendors • Marketing Vendors • Affiliates and Related Entities Sale/Sharing: N/A	• Products/Services • Customer Management • Customer Service/Communications • Payment/Financial • Serving Ads • Ads Administration • Quality and Safety • Security • Recordkeeping • Legal/Compliance • R&D • Purposes Disclosed at Collection • Legitimate Business Purposes	After no longer needed for the processing purpose(s) or after a maximum of 50 months of non-activity.
8. Audiovisual and Similar Information	Audio Visual Information, Smart Devices and Sensor Data	Disclosures for Business Purposes: • Business Vendors • Affiliates and	• Products/Services • Customer Management • Customer Service/Communications • Payment/Financial • Quality and Safety	After no longer needed for the processing purpose(s) or after a maximum of 50 months of non-

		Related Entities Sale/Sharing: N/A	• Security • Recordkeeping • Legal/Compliance • R&D • Purposes Disclosed at Collection • Legitimate Business Purposes	activity unless required by law or contract to retain.
9. Professional or Employment Information	General Demographics & Psychographics	Disclosures for Business Purposes: • Business Vendors • Affiliates and Related Entities Sale/Sharing: Third-Party Digital Businesses	• Products/Services • Customer Management • Customer Service/Communications • Payment/Financial • Serving Ads • Ads Administration • Quality and Safety • Security • Recordkeeping • Legal/Compliance • R&D • Purposes Disclosed at Collection • Legitimate Business Purposes	After no longer needed for the processing purpose(s) unless required by law or contract to retain.
10. Non-public Education Records	Not applicable in non-HR contexts (which are not within the scope of this notice)	Not applicable in non-HR contexts (which are not within the scope of this notice)	Not applicable in non-HR contexts (which are not within the scope of this notice)	Not applicable in non-HR contexts (which are not within the scope of this notice)
11. Inferences from Collected Information	General Demographics & Psychographics, Inferred Information	Disclosures for Business Purposes: • Business Vendors • Marketing Vendors • Affiliates and Related Entities Sale/Sharing: Third-Party Digital Businesses and Retail Partners	• Products/Services • Customer Management • Customer Service/Communications • Payment/Financial • Serving Ads • Ads Administration • Quality and Safety • Security • Recordkeeping • Legal/Compliance • R&D • Purposes Disclosed at Collection • Legitimate Business Purposes	After no longer needed for the processing purpose(s) or After no longer needed for the processing purpose(s) or after a maximum of 50 months of non-activity unless required by law or contract to retain.

Sensitive Personal Data

Category of Sensitive Personal Data	Examples of Sensitive Personal Data Types within Category	Categories of Recipients	Processing Purposes	Retention Period
1. Financial Information & Account Credentials allowing access to an account	Financial Information. In addition, we may store your P&G account logins in combination with a password in our systems.	Disclosures for Business Purposes: • Business Vendors • Affiliates and Related Entities Sale/Sharing: N/A	• Products/Services • Customer Management • Customer Service/Communications • Payment/Financial • Serving Ads • Ads Administration • Quality and Safety • Security • Recordkeeping • Legal/Compliance • R&D • Purposes Disclosed at Collection • Legitimate Business Purposes	After no longer needed for the processing purpose(s) or after a maximum of 50 months of non-activity unless required by law or contract to retain or dispose of prior.
Physical & Mental Health Data	Physical and Mental Health data / condition / information that we may ask a consumer in connection with a research study or survey. It also includes information collected when consumer contacts us to report a complaint or an adverse occurring in connection with one of our products.	Disclosures for Business Purposes: • Business Vendors • Affiliates and Related Entities Sale/Sharing: N/A	• Products/Services • Customer Management • Customer Service/Communications • Serving Ads • Ads Administration • Quality and Safety • Security • Recordkeeping • Legal/Compliance • R&D	After no longer needed for the processing purpose(s).

Precise Geolocation Data	Precise geolocation data	Disclosures for Business Purposes: • Business Vendors • Marketing Vendors • Affiliates and Related Entities Sale/Sharing: N/A	• Products/Services • Customer Management • Customer Service/Communications • Payment/Financial • Serving Ads • Ads Administration • Quality and Safety • Security • Recordkeeping • Legal/Compliance • R&D • Purposes Disclosed at Collection • Legitimate Business Purpose	After no longer needed for the processing purpose(s).
Racial or Ethnic Origin	General Demographics & Psychographics	Disclosures for Business Purposes: • Business Vendors • Marketing Vendors • Affiliates and Related Entities Sale/Sharing: • Business Vendors • Marketing Vendors	• Products/Services • Customer Management • Customer Service/Communications • Payment/Financial • Serving Ads • Ads Administration • Quality and Safety • Security • Recordkeeping • Legal/Compliance • R&D • Purposes Disclosed at Collection • Legitimate Business Purposes	After no longer needed for the processing purpose(s) or after a maximum of 50 months of non-activity unless required by law to retain.
Processing of Biometric Information for the purpose of uniquely identifying a consumer	Not applicable	Not applicable	Not applicable	Not applicable
Personal Data Concerning a Consumer's Health **This personal data would not include health diagnostic information but is related to demographic or purchase data that may help us determine which products you*	Health-related Information	Disclosures for Business Purposes: • Business Vendors • Affiliates and Related Entities Sale/Sharing: Third-Party Digital Businesses and Retail Partners (in	• Products/Services • Customer Management • Customer Service/Communications • Payment/Financial • Serving Ads • Ads Administration • Quality and Safety • Security • Recordkeeping • Legal / Compliance • R&D • Purposes Disclosed at Collection	After no longer needed for the processing purpose(s) or after a maximum of 50 months of non-activity unless required by law to retain.

may be interested in.		jurisdictions where the law permits)	• Legitimate Business Purposes	
Inferences from Collected Information	Racial or Ethnic Origin General Demographics & Psychographics	Disclosures for Business Purposes: • Business Vendors • Marketing Vendors • Affiliates and Related Entities	• Products/Services • Customer Management • Customer Service/Communications • Serving Ads • Ads Administration • Quality and Safety • Purposes Disclosed at Collection • Legitimate Business Purposes	After no longer needed for the processing purpose(s) and deleted within a maximum of 24 hours after collection.

We also may disclose each category of personal data and sensitive personal data in the table to the following categories of recipients in a manner that does not constitute Sale or Sharing:

• The Consumer or to other parties at your direction or through your intentional action

• Recipients to whom personal data is disclosed for legal and similar reasons

• In addition, our Vendors and the other recipients listed in the above table may, subject to contractual restrictions imposed by us and/or legal obligations, also use and disclose your personal data for business purposes. For example, our Vendors and the other categories of recipients listed in the table above may engage subcontractors to enable them to perform services for us or process for our business purposes.

Consumer Rights Requests

As described in further detail below, subject to meeting the requirements for a Verifiable Consumer Request (defined below), we provide Consumers – which are, for clarity, residents of certain states – the privacy rights described in this section. For residents of states without Consumer privacy rights, we will consider requests but will apply our discretion in how we process such requests. For states that have passed consumer privacy laws, but are not yet in effect, we will also consider applying state law rights prior to the effective date of such laws but will do so in our discretion.

Making a Request and Scope of Requests

As permitted by the U.S. Privacy Laws, certain requests you submit to us are subject to an identity verification process ("**Verifiable Consumer Request**") as described below in the "Verifying Your Request" section below. We will not fulfill such requests unless you have

provided sufficient information for us to reasonably verify you are the Consumer about whom we collected personal information.

To make a request, please submit your request to us by one of the methods below. For further instructions on how to submit a Do Not Sell/Share/Target request, for non-cookie PI (as defined below), please go to the "Do Not Sell/Share/Target" section below.

- Calling us at **(877) 701-0404**
- Visiting our Preference Center (which can be reached by the "Your Privacy Choices" link in the footer of our websites or via the Settings menu in our mobile applications)

Some personal data we maintain about you is not sufficiently associated with enough of your other personal data for us to be able to verify that it is your particular personal data (e.g., clickstream data tied only to a pseudonymous browser ID). We do not include that personal data in response to those requests. If we deny a verified request, we will explain the reasons in our response. You are not required to create a password-protected account with us to make a Verifiable Consumer Request. We will use personal data provided in a Verifiable Consumer Request only to verify your identity or authority to make the request and to track and document request responses unless you also gave it to us for another purpose.

We will make commercially reasonable efforts to identify personal data that we collect, process, store, disclose, and otherwise use and to respond to your privacy requests. We will typically not charge a fee to fully respond to your requests; provided, however, we may refuse to act upon a request, if your request is excessive, repetitive, unfounded, or overly burdensome. If we determine that we may refuse a request, we will give you notice explaining why we made that decision.

Verifying Your Request

To help protect your privacy and maintain security, we take steps to verify your identity before granting you access to your personal data or considering your deletion request. Upon receipt of your request, we will send you a verification form by email or postal mail. To complete your request, please respond to the verification form when you receive it. To verify your identity, we may require you to provide any of the following information: Name, email address, postal address, or date of birth.

We will review the information provided as part of your request and may ask you to provide additional information via e-mail or other means as part of this verification process. We will not fulfill your Right to Know (Categories), Right to Know (Specific Pieces/Portability), Right to Delete, or Right to Correction request unless you have provided sufficient information for us to reasonably verify you are the Consumer about whom we collected personal data. The same verification process does not apply to opt-

outs of Sale or Sharing, or limitation of sensitive personal data or special category data requests, but we may apply some verification measures if we suspect fraud.

The verification standards we are required to apply for each type of request vary. We verify your categories requests and certain deletion and correction requests (e.g., those that are less sensitive in nature) to a reasonable degree of certainty, which may include matching at least two data points provided by you with data points maintained by us, which we have determined to be reliable for the purpose of verifying you. For certain deletion and correction requests (such as those that relate to personal data that is more sensitive in nature) and for specific pieces requests, we apply a verification standard of reasonably high degree of certainty. This standard includes matching at least three data points provided by you with data points maintained by us, which we have determined to be reliable for the purpose of verifying you, and may include obtaining a signed declaration from you, under penalty of perjury, that you are the individual whose personal data is the subject of the request.

If we cannot verify you in respect of certain requests, such as if you do not provide the requested information, we will still take certain actions as required by certain U.S. Privacy Laws. For example:

- If we cannot verify your deletion request, we will refer you to this U.S. State Privacy Notice for a general description of our data practices.

- If we cannot verify your specific pieces request, we will treat it as a categories request.

Authorizing an Agent

You may designate an authorized agent to submit a request on your behalf by submitting a request in the manners described above. If you are an authorized agent who would like to make a request, the U.S. Privacy Laws require that we ensure that a request made by an agent is a Verifiable Consumer Request (except Do Not Sell/Share requests) and allow us to request further information to ensure that the Consumer has authorized you to make the request on their behalf. Generally, we will request that an agent provide proof that the Consumer gave the agent signed permission to submit the request, and, as permitted under the U.S. Privacy Laws, we also may require the Consumer to either verify their own identity or directly confirm with us that they provided the agent permission to submit the request. To make a request as an authorized agent on behalf of a Consumer, click here.

Appeal Rights

You may appeal a denial of your request by clicking here.

Right to Know/Access

Right to Know–- Categories Request

You have the right to request, twice in a 12-month period, the following information about the personal information we have collected about you during the past 12 months:

- the categories of personal information we have collected about you;
- the categories of sources from which we collected the personal information;
- the business or commercial purposes for which we collected or sold the personal information;
- the categories of third parties to whom we sold or shared the personal information, by category or categories of personal information for each category of third parties to whom the personal information was sold or shared;
- the categories of personal information about you that we disclosed for a business purpose, and the categories of persons to whom disclosed that information for a business purpose.

Right to Know–- Specific Pieces

You have the right to request a transportable copy of the specific pieces of personal data we collected about you in the 12-month period preceding your request. Please note that personal data is retained by us for various time periods, so there may be certain information that we have collected about you that we do not even retain for 12 months (and thus, it would not be able to be included in our response to you). Please also note that you may be limited under your applicable state's law to making a certain number of "right to know" requests in any 12-month period.

Right to Delete

In addition, you have the right to request that we delete certain personal information we have collected from you. Please understand that P&G cannot delete personal data in those situations where our retention is required for our own internal business purposes or otherwise permitted by relevant U.S. Privacy Laws (such as fraud prevention or legal compliance). In these situations, we will retain your personal data in accordance with our records retention program and securely delete it at the end of the retention period.

Right to Correct

You have the right to request that we correct inaccuracies that you find in your personal data maintained by us. Your request to correct is subject to our verification (discussed above) and the response standards in the applicable U.S. Privacy Laws.

Right to Limit Sensitive Personal Data Processing

Certain personal data qualifies as “sensitive personal data” or “sensitive personal information” or “special category data” under U.S. Privacy Laws, which we refer to in this U.S. State Privacy Notice as “sensitive personal data or special category data”. Some U.S Privacy Laws require consent for the processing of sensitive personal data or special category data, which can be revoked, subject to certain exceptions and exemptions (for example, if the processing of your sensitive personal data or special category data is required to provide a product or service specifically requested by you). Depending on your state of residence, you have the right to revoke such consent, if applicable, and/or direct businesses to limit their use and disclosure of sensitive personal data or special category data if they use or disclose it beyond certain internal business purposes. You can make a request using the methods set forth above.

Rights as to Automated Decision-Making and Profiling

You have the right to opt-out of profiling in furtherance of decisions that produce legal or similarly significant effects. However, as discussed above , we do not carry out profiling or automated decision-making activities in a manner that requires us to provide opt-out rights.

Do Not Sell/Share/Target

Under the various U.S. Privacy Laws, Consumers have the right to opt-out of certain processing activities. Some states have opt-outs specific to Targeted Advertising activities - which California’s law refers to as “cross-context behavioral advertising”, and others simply as Targeted Advertising - which involve the use of personal data from different businesses or services to target advertisements to you. California provides Consumers the right to opt-out of Sharing, which includes providing or making available personal information to third parties for such Targeted Advertising activities, while other states provide Consumers the right to opt-out from processing personal information for Targeted Advertising more broadly. There are broad and differing concepts of the Sale of personal data under the various U.S. Privacy Laws, all of which at a minimum require providing or otherwise making available personal data to a third party.

When you provide us personal data for the below Processing Purposes, we may use some or all of that personal data to advertise to you. This may include making available your personal data collected during these Processing Purposes to third parties in way that may constitute a Sale and/or Sharing, as well as using your personal data for purposes of Targeted Advertising.

- Products/Services.

- Customer Management.

• Customer Service/Communications,

• Serving Ads.

• Ads Administration,

• Purposes Disclosed at Collection

Third-Party digital businesses, including online platforms (Google, Amazon, Facebook, etc.) and AdTech companies such as Demand Side Platforms which help us place advertisements ("**Third-Party Digital Businesses**") may associate cookies and other tracking technologies that collect personal data about you on our apps and websites, or otherwise collect and process personal data that we make available about you, including digital activity information. Giving access to personal data on our websites or apps, or otherwise, to Third-Party Digital Businesses could be deemed a Sale and/or Sharing and could implicate processing for purposes of Targeted Advertising under some U.S. Privacy Laws. Therefore, we will treat such personal data collected by Third-Party Digital Businesses (e.g., cookie ID, IP address, and other online IDs and internet or other electronic activity information) as such, and subject to the opt-out requests described above. In some instances, the personal data we make available about you is collected directly by such Third-Party Digital Businesses using Tracking Technologies on our websites or apps, or our advertisements that are served on third-party sites (which we refer to as "**cookie PI**"). However, certain personal data which we make available to Third Party Digital Businesses is information that we have previously collected directly from you or otherwise about you, such as your email address (which we refer to below as "**non-cookie PI**").

When you opt-out pursuant to the instructions below, it will have the effect of opting you out of Sale, Sharing, and Targeted Advertising, such that our opt-out process is intended to combine all of these state opt-outs into a single opt-out. Instructions for opting out are below. ***Please note that there are distinct instructions for opting out of cookie PI and non-cookie PI, which we explain further, below.***

Opt-out for non-cookie PI: If you would like to submit a request to opt-out of our processing of your non-cookie PI (e.g., your email address) for Targeted Advertising, or opt-out of the Sale or Sharing of such data, make an opt-out request here.

Opt-out for cookie PI: If you would like to submit a request to opt-out of our processing of your cookie PI for Targeted Advertising or opt-out of the Sale/Sharing of such personal data, you need to exercise a separate opt-out request on our cookie management tool. To do so, click "Do Not Sell or Share My Personal Information / Opt-Out of Targeted Advertising" in the footer of each of our websites and/or in the Settings menu of each of our mobile applications. Then follow the instructions for the toggle. This is because we have to use different technologies to apply your opt-outs of cookie PI and of non-cookie PI.

Our cookie management tool enables you to exercise such an opt-out request and enable certain cookie preferences on your device.

You must exercise your preferences separately on each of our websites that you visit, within each of our mobile applications that you use, if you use a different browser than the one on which you originally opted out, and on each device that you use. Since your browser opt-out is designated by a cookie, if you clear or block cookies, your preferences will no longer be affective, and you will need to enable them again via our cookie management tool.

For more information about how we have shared your personal data with third parties such that it constitutes a "Sale" or "Share" under CCPA during the 12-month period prior to the date this privacy policy was last updated, please refer to the chart above. We do not knowingly Sell or Share personal data of minors older than 13 years of age and under 16 years of age without their consent.

Global Privacy Control ("GPC")

Some of the U.S. Privacy Laws require businesses to process GPC signals, which is referred to in some states as opt-out preference signals and in other states as universal opt-out mechanisms. GPC is a signal sent by a platform, technology, or mechanism, enabled by individuals on their devices or browsers, that communicate the individual's choice to opt-out of the Sale and Sharing of personal data, or of processing of personal data for Targeted Advertising. To use GPC, you can download an internet browser or a plugin to use on your current internet browser and follow the settings to enable the GPC. We have configured the settings of our consent management platform to receive and process GPC signals on our website and mobile applications, which is explained by our consent management platform here.

Certain of the U.S. Privacy Laws require us to explain how we process GPC signals in detail, specifically how we apply GPC signals and the corresponding Do Not Sell/Share/Target requests to online data (what we refer to above as "cookie PI") and offline data (what we refer to above as "non-cookie PI"). Below we explain the scenarios in which we apply the Do Not Sell/Share/Target requests communicated by GPC signals to cookie PI and, where applicable, to non-cookie PI:

• When you are visiting our website on a particular internet browser ("browser 1"), we will apply the GPC signal and corresponding Do Not Sell/Share/Target to cookie PI collected on that browser 1.

• When you log in on browser 1: We will be able to apply the GPC signal and corresponding Do Not Sell/Share/Target request to non-cookie PI associated with your user account, but only if and after you have logged into your user account on browser 1.

When you visit our website on a different browser (“browser 2"). If you later visit our website on browser 2 (whether on the same device or a different device) and GPC is not enabled, we are unable to apply the prior GPC signal from browser 1 to cookie PI on browser 2, unless and until you login to your user account on browser 2. We will continue to apply the Do Not Sell/Share/Target opt-outs communicated via the GPC signal on browser 1.

We process GPC signals in a frictionless manner, which means that we do not: (1) charge a fee for use of our service if you have enabled GPC; (2) change your experience with our website if you use GPC; or (3) display a notification, pop-up, text, graphic, animation, sound, video, or any interstitial in response to the GPC.

Incentive and Loyalty Programs; Right to Non-Discrimination

Loyalty/Incentive Programs Notice

We also collect and use your personal data to administer and maintain Rewards Programs (defined above in “How We Gather & Use Personal Data”), which may be considered a “financial incentive” or a “bona fide loyalty program” under one or more of the U.S. Privacy Laws.

We use all categories of personal data disclosed in the above table, excluding “biometric information,” “professional or employment information, and “non-public education records,” to administer and maintain such Rewards Programs. All categories of personal data we use for loyalty programs may also be Sold or processed for Targeted Advertising. We may also use, Sell, and process for Targeted Advertising the categories of sensitive personal data or special category data: account information and credentials, precise geolocation data, racial or ethnic origin, and personal data concerning health. While we may collect sensitive personal data or special category data in relation to some Rewards Programs, the collection and processing of sensitive personal data or special category data is not required to participate in Rewards Programs. We use personal data to verify your identity, offer unique rewards, track your program status, and to facilitate the exchange of program points for products, promotional materials, training workshops, and other items. The categories of third parties that will receive personal data and sensitive personal data or special category data are set forth in the table above, some of which may qualify as data brokers under some of the U.S. Privacy Laws. Some U.S. Privacy Laws require us to state whether we provide Rewards Programs benefits through third-party partners; however, while we sometimes will provide you the opportunity to independently engage with third parties through our websites or apps, third parties do not provide Rewards Programs on our behalf.

You can opt-in to a Rewards Program by signing up on the applicable rewards page. If you opt-in to participate in any of our Rewards Programs, you may withdraw from participation at any time by contacting us using the contact details in this Privacy Policy or in accordance with the instructions set forth in the applicable Rewards Program’s terms and conditions.

Under certain U.S. Privacy Laws, you may be entitled to be informed as to why financial incentive programs, or price or service differences, are permitted under the law, including (i) a good-faith

estimate of the value of your personal data that forms the basis for offering the financial incentive or price or service difference, and (ii) a description of the method we used to calculate the value of your personal data. Generally, we do not assign monetary or other value to personal data. However, in the event we are required by law to assign such value in the context of Rewards Programs, or price or service differences, we have valued the personal data collected and used as being equal to the value of the discount or benefit provided, and the calculation of the value is based upon a practical and good-faith effort often involving the (i) categories of personal data collected (e.g., names, email addresses), (ii) the use of such personal data for our marketing and business purposes in accordance with this Privacy Policy and our Rewards Programs, (iii) the discounted price offered (if any), (iv) the volume of consumers enrolled in our Rewards Programs, and (v) the product or service to which the Rewards Programs, or price or service differences, applies. The disclosure of the value described herein is not intended to waive, nor should be interpreted as a waiver to, our proprietary or business confidential information, including trade secrets, and does not constitute any representation with regard to generally accepted accounting principles or financial accounting standards. We deem the value of the personal data to be reasonably related to the value of the rewards, and by subscribing to these Rewards Programs you indicate you agree. If you do not, do not subscribe to the Rewards Programs.

Non-Discrimination

You have the right not to receive discriminatory treatment for the exercise of your privacy rights described in this U.S. State Privacy Notice. We will not deny, charge different prices for, or provide a different level or quality of goods or services in a manner that is prohibited by the U.S. Privacy Laws if you choose to exercise your rights. Please note, however, that you will no longer be able to participate in Rewards Programs request to delete personal data. This is because we need the personal data collected in relation Rewards Program to carry out the functions described above.

California Consumer Request Metrics

Click here to see request metrics from the previous calendar year.

Other California Notices

California Notice for Minors

We may offer interactive services which allow teens under the age of 18 to upload their own content (e.g., videos, comments, status updates, or pictures). This content can be removed or deleted any time by following the instructions on our sites. If you have questions about how to do this, contact us. Be aware that such posts may have been copied, forwarded, or posted elsewhere by others and we are not responsible for any such actions. You will, in such cases, have to contact other site owners to request removal of your content.

California Shine the Light

We provide California residents with the option to opt-out to sharing of “personal information,” as defined by California’s “Shine the Light” law, with third parties (other than with Company

affiliates) for such third parties' own direct marketing purposes. California residents may exercise this opt-out, request information about our Shine the Light law compliance, and/or obtain a disclosure of third parties we have shared information with and the categories of information shared. To do so contact us at 1 Procter & Gamble Plaza, Cincinnati, OH 45202, U.S.A. (Attn: Privacy). You must put the statement "Shine the Light Request" in the body of your correspondence. In your request, please attest to the fact that you are a California resident and provide a current California address for your response. This right is different than, and in addition to, CCPA rights, and must be requested separately. We are only required to respond to one request per Consumer each year. We are not required to respond to requests made by means other than through the provided mail address. We will not accept Shine the Light requests by telephone or by fax, and are not responsible for requests not labeled or sent properly, or that are incomplete.

EEA, UK, Switzerland, and Serbia Privacy

This section includes information that is required to be disclosed in respect of our processing of personal data of EEA country, UK, Swiss and Serbian residents. It aims to provide increased transparency into our processing, retention, and transfer of EEA, UK, Swiss and Serbian residents personal data that is in line with the letter and spirit of the General Data Protection Regulation ("GDPR"), the Swiss Federal Act on Data Protection, the Serbian Law on Personal Data Protection and the GDPR as incorporated into UK law by the Data Protection Act 2018 and amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019. Certain information, such as the Entities and list of Data Controllers below. The retention periods described above, however, apply more broadly to personal data of residents of the states described above in the U.S. State Privacy Notice.

Entities

Different P&G entities may be the controller of your personal data. A data controller is the entity which directs the processing activity and is principally responsible for the data. The chart below identifies our data controllers for EEA country, UK and Serbian data. For example, when you register for email on one of our French websites, the P&G entity listed next to that country name will be the controller of that personal data (e.g., Procter & Gamble France SAS).

The data controller for the Smart Sleep Coach application is P&G Baby Care Digital LLC, located at One Procter & Gamble Plaza, Cincinnati, Ohio, 45202.

Countries	Data Controller
Austria	Procter & Gamble Austria – Zweigniederlassung der Procter & Gamble GmbH, Wiedner Gürtel 13, 100 Wien
Belgium	Procter & Gamble Distribution Company (Europe) BV

	For P&G Healthcare: P&G Health Belgium BV, Temselaan 100, 1853 Strombeek-Bever
Bulgaria	Procter & Gamble Bulgaria EOOD, Sofia 1404, Bd. Bulgaria nr. 69, Bulgaria
Croatia	Procter & Gamble d.o.o. za trgovinu, Bani 110, Buzin, 10010 Zagreb, Croatia
Czech Republic	Procter & Gamble Czech Republic s.r.o., 269 01 Rakovnik, Ottova 402, Czech Republic
Denmark	Procter & Gamble Danmark ApS Stensmosevej 15, stuen. 2620 Albertslund, Denmark
Estonia	Procter & Gamble International Operations SA, Route de Saint-Georges 47 1213 PETIT-LANCY Geneve
Finland	Procter & Gamble Finland Oy, Lars Sonckin Kaari 10, 02600 ESPOO, Finland
France	Procter & Gamble France SAS For P&G HealthCare: P&G Health France SAS 163/165 quai Aulagnier, 92600 Asnières-sur-Seine
Germany	Procter & Gamble Service GmbH, Sulzbacher Strasse 40, 65824 Schwalbach am Taunus For P&G Health: P&G Health Germany GmbH, Sulzbacher Strasse 40, 65824 Schwalbach am Taunus
Greece	P&G Hellas Ltd. 49 Ag. Konstantinou str., 15124 Maroussi – Athens, Greece
Hungary	1097 Budapest, Könyves Kálmán krt. 34., Hungary
Ireland	Procter & Gamble UK, The Heights, Brooklands, Weybridge, Surrey KT13 0XP
Italy	Procter & Gamble Srl, viale Giorgio Ribotta 11, 00144 Roma
Latvia	Procter & Gamble International Operations SA, Route de Saint-Georges 47 1213 PETIT-LANCY Geneve
Lithuania	Procter & Gamble International Operations SA, Route de Saint-Georges 47 1213 PETIT-LANCY Geneve
Netherlands	Procter & Gamble Nederland B.V., Watermanweg 100, 3067-GG Rotterdam New address as of April 27, 2020: Weena 505, 3013 AL Rotterdam
Norway	Procter & Gamble Norge AS Visiting address: Nydalsveien 28, 0484 Oslo Postal address: Postboks 4814, 0422 Oslo

Poland	Procter and Gamble DS Polska sp z o.o., ul. Zabraniecka 20, 03-872 Warszawa, Poland
Portugal	Procter & Gamble Portugal, Productos de Consumo Higiene de Saúde, S.A., S.A. Edificio Alvares Cabral 3º, Quinta da Fonte, 2774-527 Paço D'Arcos, Portugal
Romania	For contests: Procter & Gamble Distribution SRL, 9-9A Dimitrie Pompei Blvd., Building 2A, District 2, Bucharest 020335, Romania For other sites: Procter & Gamble Marketing Romania SR, 9-9A Dimitrie Pompei Blvd., Building 2A, District 2, Bucharest 020335, Romania
Serbia	Procter & Gamble Doo Beograd, Španskih boraca 3, 11070 Novi Beograd, Belgrade, Serbia
Slovakia	Procter & Gamble, spol. s.r.o., Einsteinova 24, 851 01 Bratislava, Slovakia
Spain	Procter & Gamble España, S.A.U., Avenida de Bruselas, 24, 28108 Alcobendas, Madrid, Spain
Sweden	Procter & Gamble Sverige AB Visiting address: Telegrafgatan 4, 169 72 Solna, Sweden Postal address: Box 27303, 102 54 Stockholm
United Kingdom	Procter & Gamble UK Seven Seas Limited, The Heights, Brooklands, Weybridge, Surrey KT13 0XP

Colombia Privacy

Procter & Gamble Colombia Ltda., with NIT. 800.000.946-4, address at Carrera 7 # 114-33, 12th floor, Bogotá D.C., with phone number: 601-5280000 and email address notifications.im@pg.com, acting as the Data Controller, and in compliance with articles 15 and 20 of the Constitution of Colombia, Law 1581 of 2012, Law 1266 of 2008, Decree 1377 of 2013, and Decree 1074 of 2015, informs all data subjects that the personal data provided will be processed in accordance with the purposes described in this privacy Policy https://privacypolicy.pg.com/es-co/.

Rights of the Owner of personal data residing in Colombia

In compliance with articles 15 and 20 of the Constitution of Colombia, Law 1581 of 2012, Law 1266 of 2008, Decree 1377 of 2013, and Decree 1074 of 2015, data subjects are informed that the personal data provided will be processed in accordance with the purposes described in this privacy policy. Likewise, it is informed that data subjects have the following rights: a) to know, update, and rectify their personal data regarding partial, inaccurate, incomplete, fractioned, misleading, or data whose processing is expressly prohibited or has not been authorized; b) to request proof of the authorization granted, unless expressly exempted as a requirement for processing; c) to be informed, upon request, of the use that has been

given to their personal data; d) to file complaints with the Superintendence of Industry and Commerce for violations of Law 1581 of 2012 and other regulations that modify, add, or complement it; e) to revoke the authorization and/or request the deletion of the data when the processing does not comply with constitutional and legal principles, rights, and guarantees. The revocation and/or deletion will proceed when the Superintendence of Industry and Commerce has determined that the Data Controller or Processor have engaged in conduct contrary to this law and the Constitution; f) to access their personal data that have been subject to processing free of charge. The aforementioned rights may be exercised in accordance with the provisions set forth in this section and the privacy policy, which can be found at the following link: https://privacypolicy.pg.com/es-co/.

Authorization and form of collection of personal data

For the processing of personal data, Procter & Gamble Colombia Ltda. will obtain the prior, express, and informed consent of the data subject. This consent may be obtained through any means that can be consulted later and may be granted through different mechanisms enabled by Procter & Gamble Colombia Ltda., in writing, orally, or through the data subject's unequivocal conduct.

The data subject's consent will not be necessary when it concerns:

- Information required by a public or administrative entity in the exercise of its legal functions or by judicial order.
- Data of a public nature.
- Cases of medical or sanitary urgency.
- Processing of information authorized by law for historical, statistical, or scientific purposes.
- Data related to the Civil Registry of Persons.

Processing of personal data

Procter & Gamble Colombia Ltda uses personal data to fulfill the purpose of affecting and improving people's lives, better understanding their interests and preferences as consumers and individuals. We use your information for the processing purposes designated in the privacy policy, which can be found at the following link: https://privacypolicy.pg.com/es-co/, and for the following purposes:

- Carrying out marketing, promotion, and/or advertising activities through different means such as personal visits to customers, marketing, and sending information by

physical and electronic means.

- Providing customers with information that allows them to access offers, promotions, discounts, launches, and supplying information of interest (personalized attention, benefits, use, health care, and well-being, etc.).
- Fulfilling obligations contracted with customers, suppliers, and employees.
- Informing about changes to our products and/or services.
- Evaluating the quality of products and/or services and measuring customer satisfaction.
- Disseminating policies, programs, results, and organizational changes.
- Analyzing information for the development and implementation of commercial or marketing strategies, as well as designing, implementing, and developing programs, projects, and events.
- Contacting the data subject through calls, text messages, emails, and/or physical means for activities related to the authorized purposes.
- Electronic invoicing.
- Disclosing, transferring, and/or transmitting personal data within and outside the country to Procter & Gamble Colombia Ltda.'s parent companies, subsidiaries, or affiliates, or to third parties because of a contract, law, or lawful relationship requiring it or to implement cloud computing services, with the same limitations and rights.
- Transferring and/or transmitting sensitive personal data to competent public entities, either by virtue of a legal mandate or judicial or administrative order, on account of or suspicion of adverse events that Procter & Gamble Colombia Ltda. has become aware of, relating to technical claims or others.
- Knowing, storing, and processing all the information provided in one or more databases, in the format that Procter & Gamble Colombia Ltda. deems most convenient.
- Managing procedures (requests, complaints, claims).
- Sending information regarding the use and care of offered products, whether directly or through the data processor.
- The attention of requests, complaints or claims (PQR) related to the activity and/or products of P&G.

International Transfer and Processing of Personal Data

Procter & Gamble Colombia Ltda. carries out International Transfer of personal data to other parent companies, affiliates or subsidiaries or with service providers that may store, process or access the data, as a consequence of a contract, law or legal link that requires it. To carry out this process, Procter & Gamble Colombia Ltda. has verified that the transfer or transmission of personal data will be carried out to countries that meet the standards that guarantee an adequate level of protection of personal data, in accordance with the provisions of article 26 of Law 1581 of 2012 and section 3.2. of Chapter Three, of Title V of the Sole Circular of the Superintendence of Industry and Commerce.

Additionally, Procter & Gamble Colombia Ltda. may also carry out the Transmission of personal data through different management software whose servers are located in a country other than Colombian territory, the above in order to manage all the internal processes of Procter & Gamble Colombia Ltda. In any case, in addition to having express and unequivocal authorization from the Owner, Procter & Gamble Colombia Ltda. will ensure that the action provides adequate levels of data protection. and meets the requirements established in Colombia by the Habeas Data Regime.

Personal Data of Children and Adolescents

Procter & Gamble Colombia Ltda. may collect public data from children and adolescents for specific activities, always respecting the best interests of the minor and the prevailing rights of children and adolescents enshrined in article 44 of the Political Constitution of Colombia. For this purpose, Procter & Gamble Colombia Ltda. will have prior authorization granted by the guardian or parents of the minor.

In any case, personal data collected from children and adolescents will not be used for targeted advertising.

Attention to inquiries, complaints, revocation of authorization, updating, withdrawal, correction, or deletion of databases (generally known as "PQRS").

The data subject, their successors, representatives, or anyone determined by stipulation in favor of another (generally known as the "Interested Party") may exercise their rights by contacting us through written communication addressed to the customer service department.

The communication can be sent through one of the following channels:

- Email: to send an email click HERE

- Telephone: 01-800-917-0036
- Written communication submitted to Carrera 7 # 114-33, 12th floor, Bogotá D.C.
- Preference Center click HERE

Procedure for the exercise of queries, requests, complaints, revocation of authorization, updating, withdrawal, correction, or deletion of databases

Verification of the Data Subject's identity and the content of any request

To help protect the privacy and security of the Data Subject, we take steps to verify their identity before responding to the request. Therefore, to address your request, we ask you to provide the Data Subject's identification data:

- Full name.
- Identification number.
- Contact information (physical and/or electronic address and contact telephone numbers).
- Date of birth.

In the event that the request is submitted through our Preference Center, upon receiving your request, we will send a verification form via email. To complete the request, the Data Subject must respond to the verification form upon receipt.

Likewise, any other Interested Party who is not the Data Subject must prove their identity and their status as their successor in interest, representative, or the representation or stipulation in favor of another or for another.

For further reference on the aforementioned identity verification, please refer to the privacy policy located at the following link: https://privacypolicy.pg.com/es-co/

Taking into account the above, requests related to the processing of Personal Data must contain at least:

- The Data Subject's identification data (full name, identification number, contact information, and date of birth).
- Accreditation of the Interested Party's identity and status, if applicable (identification data and documents proving their identity and status as Interested Party).
- Means to receive a response to the request.
- Reasons and facts that give rise to the request.

- Documents intended to be invoked.

- Clear and precise description of the personal data regarding which the Data Subject seeks to exercise their right to complaint, request for rectification, updating, or deletion of their personal data (not applicable to the filing of inquiries).

Inquiry procedure

The Interested Party may submit a request indicating the information they wish to know, and in any case, inquiries will be answered within a maximum period of ten (10) business days from the date of receipt. If it is not possible to address the inquiry within said period, the Interested Party will be informed, before the expiration of the ten (10) business days, of the reasons for the delay and the date on which the inquiry will be addressed, which in no case may exceed five (5) business days following the expiration of the initial term.

Procedure for complaints, revocation of consent, withdrawal, correction, updating, or deletion of personal data

When the Data Subject considers that the processed information should be subject to correction, updating, or deletion, or when they become aware of the alleged breach of any of the duties contained in the Law, the Data Subject or another Interested Party may submit a complaint, request for rectification, updating, or deletion of their personal data.

If the complaint is incomplete, the Interested Party will be given a period of five (5) days following the receipt of the complaint to remedy any deficiencies. If two (2) months have passed since the date of the request without the applicant providing the requested information, it will be understood that they have withdrawn the complaint.

In the event that Procter & Gamble Colombia Ltda. receives a complaint that it is not competent to resolve, it will forward it to the appropriate authority within a maximum period of two (2) business days and inform the Data Subject.

The maximum period to address the complaint will be fifteen (15) business days from the day following the date of its receipt. If it is not possible to address the complaint within said term, the interested party will be informed of the reasons for the delay and the date on which their complaint will be addressed, which in no case may exceed eight (8) business days following the expiration of the initial term.

Modification of Policies

Procter & Gamble Colombia Ltda., reserves the right to modify this Personal Data Treatment and Protection Policy at any time. However, any modification will be communicated to the owners of the personal data through an efficient means and prior to its implementation.

In the event that a Personal Data Owner does not agree with the modification to the Data Processing Policy, the Owner may request Procter & Gamble Colombia Ltda. to withdraw or delete their personal data.

Validity

This policy is effective as of February 14, 2024, and was updated as March 10, 2025. Any updates once approved will be duly communicated to the Data Subjects.

The databases in which personal data will be registered will remain valid until you request the deletion of personal data or withdraw your consent. Otherwise, we will delete your personal data from our databases after they are no longer necessary for the purpose of the processing described in this section or after a maximum of 50 months of inactivity, unless the law or contract requires us to keep them for a longer period.

We define inactivity through various internal criteria that indicate a lack of interaction by a user with our programs and communications. For example, if you do not log in or do not open or click on our emails, we will consider you "inactive" and delete your data after a maximum of 50 months, but earlier for certain countries according to local legal requirements. We may need to retain some personal data to fulfill your requests, including continuing to keep you opted out of marketing emails or to comply with other legal obligations. We may also retain certain personal data used in ratings and reviews for as long as the review is used or until the product is discontinued.

Malaysia Privacy

This notice supplements the Global Privacy Policy above (the "Privacy Policy").

Data Protection Officer

If you have any questions or concerns about your Privacy and our data protection practices, you can contact our Data Protection Officer using the following channels:

Email: MYDataprivacy@shared.pg.com

Phone: 03 7724 3200

Written Communication can be sent to: Procter & Gamble (Malaysia) Sdn Bhd, 10th Floor, Surian Tower, No. 1, Jalan PJU 7/3, Mutiara Damansara, 47810 Petaling Jaya, Selangor

Nigeria Privacy

Reporting a potential data breach to P&G

Personal data breach means a breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Confirmed or suspected data breaches should be reported promptly to P&G's Data Protection Officer. All data breaches will be logged by the Data Protection Officer to ensure appropriate tracking of the types and frequency of confirmed incidents for management and reporting purposes.

An individual who wishes to complain about how their personal information may have been breached may lodge their complaint directly with the Data Protection Officer by email: nigeriadpo.im@pg.com.

The complaint should include:

- a detailed description of the security incident that caused the data breach,
- the type of personal data that was affected by the data breach,
- the identity of the affected person,
- and any other information that may be requested by the Data Protection Officer.

Any such complaints should be reported within 72 (seventy-two) hours of the occurrence of the suspected or confirmed data breach.

Reporting a data breach to the authorities

P&G will seek to report potential data breaches within 72 hours of knowledge of such breaches to the relevant authorities responsible for monitoring the security of personal data.

Saudi Arabia Privacy

This notice supplements the Global Privacy Policy above (the "**Privacy Policy**"). Terms which appear capitalized but ae not defined in the Policy or in the Notice have the meaning given under the Personal Data Protection Law promulgated by Royal Decree No. M/19, dated 09/02/1443H on 24 September 2021

Data Controller

Ismail Abudawood and Procter & Gamble Limited

Modern Products Company Limited

Categories of Personal Data & Legal Basis for Processing

In Saudi Arabia, 'Sensitive Data' includes personal information revealing racial or ethnic origin, or religious, intellectual, or political belief, data relating to security criminal convictions and offenses, biometric or Genetic Data for the purpose of identifying the person, Health Data, and data that indicates that one or both of the individual's parents are unknown.

Our legal basis for processing personal data are set out in the Privacy Policy. Where we process Sensitive Data, we will always obtain explicit consent as required by law.

How We Collect Personal Data

When we collect personal data from third parties, we do so in accordance with the Privacy Policy and only to the extent permitted by applicable law.

How we Disclose Personal Data

When we disclose personal data to third parties, we do so in accordance with the Privacy Policy as well as the applicable requirements under the law.

International Transfers

We may transfer your personal data to countries outside Saudi Arabia as set out in the Privacy Policy above. When doing so, we are complying with all applicable requirements under applicable law to protect personal data transferred outside Saudi Arabia adequately. This includes transferring your data to countries that are recognized by the competent authority as adequately protecting personal data or implementing certain additional and appropriate safeguards to protect personal data (as required by applicable law).

Data Subject Rights

You have the right to access the personal data we hold about you, the right to request access to such personal data in a readable and clear format, the right to request correction of personal data where you believe it is inaccurate, and the right to request destruction of personal data (in certain circumstances). You may also withdraw your consent at any time where we are relying on your consent to process your personal data. To exercise your rights, click here or send us an email by clicking here.

If you are not happy with our response to your requests, you have the right to lodge a complaint with the data protection regulator, the Saudi Data & Artificial Intelligence

Authority (“SDAIA”). You can contact SDAIA using the following details:

Website: https://sdaia.gov.sa

Phone: +966 11 223 2222

Vietnam Privacy

As a data subject, you have the rights related to your data as provided by Vietnam regulations, such as: right to be informed, to give and withdraw consent, requests for access, erasure, rectification/correction, to restrict personal data processing, to object to our use of your personal data for advertising, to self-protection or request other competent organizations/agencies to protect your rights. You are obliged to provide complete and accurate personal data when consenting to the processing of personal data, as well as other obligations according to applicable data privacy laws.

Some of the personal data we collect are considered sensitive personal data under applicable laws, which might include: race and ethnicity, location data of the individual identified through location services; other data that can directly or indirectly indicates your physical location such us IP address, Health-related Information, Bank Account Information, and Biometric Information.

Please note that Legitimate Interest is not the only legal requirement for personal data processing in Vietnam, and we will seek your consent to process personal data unless other exceptions apply as provided by laws.

We only collect and process personal data of children under 16 years of age after we have obtained the consent of the children, if aged seven or older, and of their parent/legal guardian, unless otherwise provided by applicable laws.

In case of a data breach, we will comply with all reporting and remedial obligations under applicable laws.

Contact Us

Still have a question or concern? We’re here to help.

Please contact us directly with any questions or concerns you may have about your privacy and our data protection practices or if you are a consumer with a disability and need a copy of this notice in an alternative format. If you have an inquiry that is specific to our data protection officer, such as a suspected data breach, please contact us here and state that in your message. You may also write to our Data Protection Officer at 1 Procter & Gamble Plaza, Cincinnati, OH 45202, U.S.A.

Art. 27 GDPR Representative:

The contact details of our Art. 27 GDPR representative in the UK and EU are as follows: Procter & Gamble Ireland, The Graan House, Units E1 and E14, Calmount Business Park, Dublin 12, Ireland

---