



Global External Party Resources Privacy Notice

Privacy Notice Contact:	Global Data Protection Officer (pgprivacyofficer.im@pg.com)	Date:	June 18th, 2026
Region:	Global	Scope:	All External Party Resources

1.0 Intent

This Notice informs all External Party Resources (“EPRs”) (defined below) of how The Procter & Gamble Company, its subsidiaries and/or affiliates (“P&G” or the “Company”) will collect and manage your Personal Information.

2.0 Independent Contractor Status

This Notice does not create an employment relationship between P&G and an EPR. EPRs provide services to P&G as independent contractors, regardless of whether such services are provided directly to P&G, or by virtue of an agreement between P&G and the EPR’s employer.

3.0 Definitions

External Party Resource: Any individual providing P&G with work or services for whom P&G is not the employer of record at the time the work or services are provided, such as contractors.

Personal Information: Any information relating to an identified or identifiable individual, such as their name, other identifiers, contact details, professional information, and personal characteristics.

The Company or P&G: For purposes of this notice, the Company or P&G refers to The Procter & Gamble Company, its subsidiaries and/or affiliates.

4.0 Principles

P&G’s fundamental data privacy processing principles are:

- Collect and manage the minimum amount of EPR Personal Information.
- Respect individual privacy.
- Comply with our Purposes, Values and Principles (PVPs), this Notice and relevant laws.
- Follow appropriate standards and procedures when collecting and/or managing EPR Personal Information.

5.0 Notice

P&G respects your privacy. This Notice describes how we process EPR Personal Information, the types of information we collect directly from you and/or from your employer, the purposes for which we use it, the categories of recipient with whom we share it, and the choices you can make about our use of it. We also describe the measures we take to protect the security of EPR Personal Information and how you can contact us about our privacy practices.

5.1 For What Purposes Do We Collect and Use EPR Personal Information?

P&G collects Personal Information about its EPRs in the context of the services agreement and independent contractor relationship P&G has with you and/or your employer. We generally collect

and use EPR Personal Information from you and/or from your employer for the following services and/or activities:

- Occupational health/safety, including health-related screenings and medical programs related to COVID-19 or similar health emergencies
- Site access management
- Identity and credential management, including identity verification and authentication, issuing ID cards and badges, system administration, recording log in/out, and management of access credentials, information security and cybersecurity
- Contingency planning purposes, including business continuity, staffing, shift management and emergency/safety protocols
- Electronic device enrollment and management, and network and device usage optimization
- Physical and cyber security controls, including electronic device and network monitoring and security video recording such as CCTV
- Litigation and internal/external investigations, audits, and dispute resolution
- Daily work processing (e.g., authenticating and logging into our systems)
- Participation in meetings, trainings and events
- Compliance with laws, regulations and Company policies regarding antibribery, child labor, anticorruption, sanctions, export controls, human rights and other corporate governance and stewardship requirements
- Investigations led by P&G and/or your employer regarding workplace misconduct or process violations
- Enforcement and auditing of our service agreements with you and/or your employer, including assessing the performance of the services,
- Compliance with all legal, regulatory, judicial or governmental requirements and responding to and complying with court orders, subpoenas, discovery requests, or other governmental data requests
- Security and risk management, including security and monitoring of personnel and premises, and protecting P&G, our workers and our clients against theft, legal liability, fraud or abuse.

5.2 What Types of EPR Personal Information Do We Collect?

We will always minimize the types and amount of EPR Personal Information we collect from or about you. The chart below describes in more detail the categories of EPR Personal Information that P&G collects in connection with its business processes.

The collection of information and access to information will vary depending on country-specific legal and/or business requirements.

The legal or business basis for collecting and processing EPR Personal Information will vary by data type and intended use, as described in Section 5.3 below.

Which Types of EPR Data Do We Collect and Process?	Why Do We Collect and Process This Type of EPR Personal Information?
	<i>We collect and process these data types for multiple organizational and business processes as detailed in Section 5.1, and as further explained below:</i>

<u>Contact Information and Personal Characteristics</u> • Full name or previous names (such as maiden names) • Other unique identifiers, such as P&G-issued identification numbers or credentials (e.g., email log-in) or any identification number issued by your employer. • Physical/mailling address • Email address • Phone number	• Site and electronic network access • Communications with you related to business contingency planning, including shift management • Participation in meetings, trainings and events • Daily work processing (e.g., authenticating and logging into our systems) • Legal and policy compliance • Corporate governance and stewardship • Required external reporting • Investigations and incident management • Security and risk management, including security and monitoring of personnel and premises, and protecting P&G, our workers and our clients against theft, legal liability, fraud or abuse • Occupational health/safety, including health-related screenings and medical programs related to COVID-19 or similar health emergencies • Enforcement and auditing of our service agreements with you and/or your employer, including assessing the performance of the services • Compliance with all legal, regulatory, judicial or governmental requirements and responding to and complying with court orders, subpoenas, discovery requests, or other governmental data requests
<u>Government ID/Work Eligibility Information/Employer ID</u> • National ID (such as passport, visas, social security number, driver's license, other government-issued identifications) • Citizenship • Residency • Nationality • Country of birth • Military and/or veteran status • Unique ID as employee of the company P&G has contracted with	• Legally identifying you and maintaining the integrity of our records • Complying with immigration and other work permit requirements • Security and risk management, such as collecting driver's license data for EPRs that operate Company automobiles, professional license verification, fraud prevention and similar purposes • Legal and policy compliance • Corporate governance and stewardship • Security and contingency planning • Required external reporting • Investigations and incident management
<u>Financial information</u> • Bank account number and details • Personal payment card information, if provided for reimbursement	• Facilitating expense reimbursement • Legal and policy compliance • Corporate governance and stewardship • Security and contingency planning

	• Required external reporting • Investigations and incident management
<u>Health Information</u> • Information related to the physical or emotional health of an individual, including any disabilities or limitations to perform work duties or functions • Drug testing and other types of health examinations	• Complying with occupational health and workplace safety and government reporting requirements • Managing EPR safety and business risks associated with the COVID-19 pandemic, or similar health emergencies • Legal and policy compliance • Corporate governance and stewardship • Security and contingency planning • Required external reporting • Investigations and incident management
<u>Electronic Identification Data/ Unique Identifiers / Image & Voice</u> • P&G system identifiers (e.g., usernames or online credentials) • Digital signature • Electronic identification data, logs and records regarding access and use of P&G devices, systems, applications, licenses, databases and the P&G network (such as your use of email, the internet, and social media). • Information collected by P&G security systems, including Closed Circuit Television ("CCTV"), site access systems, line process or task cameras • Electronic identification data, logs and records regarding access to physical P&G sites and access-restricted areas, including badge number/badge identifier and photograph • Video, photographs and other image/voice recordings in the context of meetings/trainings • Electronic identification data regarding call center recordings	• System administration, technology and IT asset access and management • Supporting our physical security, information security and cybersecurity interests against internal and/or external threats • Managing loss prevention and recovery in our offices and manufacturing sites • Internal record-keeping and reporting, including data matching and analytics • Enabling access to P&G sites, network, tools, applications and other Company systems and assets • Driving visibility on the use and costs for consumption of P&G tools, licenses, services and applications for optimization, quality, audit and cost purposes • Memorializing trainings and meetings • Legal and policy compliance • Corporate governance and stewardship • Security and contingency planning • Required external reporting • Investigations and incident management
<u>Cookies</u> - 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. Cookies do not collect any information stored on your computer or device or in your files. Cookies do not contain any information that would directly identify you. Cookies show your computer and device only as randomly assigned numbers and letters	We use cookies in P&G EPR-facing websites for a number of reasons, such as: ▪ to learn more about the way you interact with our websites and P&G content ▪ to help us improve your experience when visiting our websites ▪ to customize the website to your preferences ▪ to identify errors and resolve them

(e.g., cookie ID ABC12345) and never as, for example, John E. Smith. These are the types of cookies we use: ▪ <i>Session Cookies.</i> Session cookies remember you (using a randomly generated ID) as you move from page to page, so that you don't get asked to provide the same information you've already provided. These cookies are deleted as soon as you leave our site or close your browser. ▪ <i>Persistent Cookies.</i> Persistent 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. ▪ <i>Analytics Cookies.</i> These cookies tell us how our websites are working. In some 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.	▪ to analyze how well our websites are performing
<u>Other Personal Characteristics</u> • Biometric information including facial recognition data and mathematical representations of biometric identifiers, fingerprints or other facial scans • Criminal history/background checks	• Facilitating your access to Company sites and systems, as well as enabling productivity or collaboration tools in meeting software such as transcription, via biometric data • Legal and policy compliance • Corporate governance and stewardship • Security and contingency planning • Required external reporting • Investigations and incident management

5.3 Under What Legal and/or Business Basis Do We Process EPR Personal Information?

We collect and manage the minimum EPR Personal Information needed to: comply with our contractual and/or legal obligations related to our independent contractor relationship with you and/or your employer; to support the Company's legitimate business interests in a manner that is proportional to your privacy interests; and to process Personal Information provided with your consent, when applicable, for its intended purposes.

The legal and/or business basis for processing EPR Personal Information may be P&G's compliance with applicable laws and regulations; compliance with its contractual obligations; the Company's legitimate business interests; public health interests; and/or your consent.

The legal and/or business basis for processing EPR Personal Information may vary by jurisdiction, as well as by the data category/type and the reasons why we collect and use such information.

These are the legal bases we will generally rely on for the processing of these categories of data:

Type of Personal Data	Legal/Business Basis for Processing
Contact Information, Government ID, Financial Information, Health Information	P&G's compliance with contractual and legal obligations
Government ID / work eligibility	P&G's compliance with applicable laws
Professional Data, Contact Information	P&G's legitimate business interests

5.4 How Do We Share EPR Personal Information?

P&G will only share EPR Personal Information with those who have a legitimate business need to know.

P&G may share your information with your employer (and other entities when instructed by your employer), P&G contractors, suppliers, agencies, temporary workers, or any other parties acting on P&G's behalf ("External Parties").

EPR Personal Information may be shared with our headquarters and affiliates globally as necessary to achieve the processing purposes set out under Section 5.2 above.

We may also disclose EPR Personal Information if we are required to do so by law or legal process; to enforce or protect the rights and policies of P&G; and/or to assist in the investigation of suspected or actual misconduct or illegal activity.

5.5 What Are Your Privacy Rights?

You have the right to contact us and request access to the EPR Personal Information that we process about you. Where permitted by applicable law you may request that inaccurate, outdated or unnecessary information be corrected, erased, or restricted, as well as ask P&G to provide your data in a format that allows you to transfer your data to a service provider as appropriate in the circumstances. Where the processing of EPR Personal Information is based on consent, you have the right to withdraw your consent at any time. Where the processing of EPR Personal Information is based on legitimate interest, you have the right to object to the data processing under certain circumstances.

When exercising these rights, we encourage you to first discuss your concerns with the P&G employee who serves as your site sponsor. Alternatively, you may contact our Data Protection Officer at the address below. If you are not happy with our response to your request or our processing of your Personal Information, you may lodge a complaint with the data protection authority in your country.

5.6 How Do We Transfer EPR Personal Information?

P&G is a global business and has EPRs in many countries. If legally permitted, and subject to country-specific requirements and/or limitations, EPR Personal Information may be transferred to countries outside of the country in which it was collected. EPR Personal Information may be stored in systems in the United States, accessed from other P&G affiliates worldwide, including their service providers, or transferred to other countries as necessary to conduct relevant business operations. Those countries may not have the same data protection laws as your country of residence. When your Personal Information is transferred to or accessed from countries outside your home country, we

implement appropriate safeguards, as well as any legally required administrative, technical, and/or contractual requirements, to protect your it. We perform transfers outside of the European Economic Area (EEA), United Kingdom (UK) and Switzerland, both between P&G entities and to our service providers in reliance on the Standard Contractual Clauses. If you would like a copy of these Clauses, contact corporateprivacy.im@pg.com. P&G will also comply with other country-specific requirements that restrict data transfers outside of the country of collection.

5.7 How Do We Secure EPR Personal Information?

We implement appropriate physical, administrative, and technical measures, such as pseudonymization, encryption and access controls, designed to protect EPR Personal Information against accidental, unlawful, or unauthorized destruction, loss, alteration, disclosure or access or use, and all other unlawful forms of processing. Where External Parties process EPR Personal Information on P&G's behalf, we also enter contracts with those External Parties to ensure they are implementing the appropriate physical, administrative, and technical measures in handling such data.

5.8 How Long Do You Keep my Personal Information?

We keep EPR Personal Information for as long as necessary to fulfill the purposes for which it was collected, unless a longer retention period is required or permitted by applicable law. This will generally be for the period that you provide use with services. In some cases, we may need to retain EPR Personal Information for a period of time after the termination of your relationship with P&G in order to comply with legal or contractual obligations.

We will retain this biometric data for no more than three years from the last interaction with us, unless we are required to retain it longer for legal or regulatory compliance purposes, or to exercise or defend our legal interests. We have implemented commercially reasonable protocols to safeguard and, when appropriate, to permanently delete or dispose of such biometric data.

5.9 Does P&G Monitor Network and Device Usage?

The Company monitors P&G network and P&G device usage. P&G has an obligation to protect its employees, assets, and facilities. P&G monitors its corporate networks and devices for three purposes: i) to protect the security (encompassing confidentiality, integrity, and availability) of P&G people, data, network, assets, facilities, reputation and competitive interests; ii) to investigate suspected or confirmed misconduct or violations of law (including in support of litigation); and iii) to ensure the integrity of business processes and financial reporting.

P&G does not monitor the P&G network and devices of a specific individual unless there is a legitimate reason, or we are required to so by law, including at the request of law enforcement. We reserve the right, subject to applicable law, to access, inspect, disclose, and dispose of any electronic files, data, and messages created, stored, sent, or received through our networks and devices as necessary for the purposes mentioned above. This monitoring is always compliant with relevant laws and regulations. P&G will implement additional procedures, standards, policies, and/or any active measures wherever needed to meet local legal requirements.

Specifically, P&G will conduct passive and active monitoring of P&G networks and P&G owned devices assigned to EPR's to flag potential threats to P&G interests. The "passive monitoring" will not actively examine an individual's behavior, but instead looks for indicators of risks. These risk indicators are predefined by P&G and specialized security vendors and are tuned to meet P&G's security needs. When such a risk indicator is triggered (an "Event"), the systems log the related data

and hold it for subsequent review and or/ investigation. Specifically, the below passive monitoring techniques will be used across P&G networks and P&G owned devices assigned to EPR's:

1. **Usage Pattern Monitoring** is a monitoring technique where software or hardware checks P&G's de-identified network and web data for a predefined set of risk indicators. This technique looks for suspicious patterns in how P&G's network and/or P&G owned devices assigned to EPR's are being *used*. For example, P&G can set the Usage Pattern Monitoring tool to look for risk indicators by P&G login location. P&G Security can tune the tool so that it will generate an alert if a user's login credentials are entered into two different P&G locations faster than a person could reasonably travel between those locations.
2. **Inbound Traffic Scanning** is a monitoring tool that scans inbound web-based communications (including email) for risk indicators as they enter P&G's network. Anti-virus and firewall software is the most common example of this tool as it continually scans inbound traffic for indicators of malware on attachments, links, websites, etc.
3. **Periodic Scanning** is a monitoring tool that scans at the P&G network and P&G device level to catch specific risk indicators that may have slipped past the perimeter scans of Inbound Traffic Scanning. This tool is useful because sometimes Events are easier to identify when viewed with additional context. An anti-virus full disk scan is a prime example of this capability.
4. **Outbound Traffic Scanning** P&G has the capability to scan outbound web traffic for specific, pre-defined risk indicators. The tool scans the outbound traffic to see if an Event is triggered according to the specified risk indicator rules. For example, P&G can write a rule that will flag large file uploads to places outside of the P&G network that include Highly Restricted data or certain keywords, like a specific chemical compound used in a new product formula

P&G assesses, based upon the nature of a risk that was flagged by the passive monitoring tools or was otherwise brought to P&G's attention (e.g., lawsuit, alleged misconduct, law enforcement, etc.), whether further investigation/analysis of the risk is required. In that assessment, P&G considers the potential harm to employees, consumers, other stakeholders, and/or the Company as well as the legal and privacy interests of any individuals involved. P&G may also determine whether further analysis is required based on legal or policy requirements to safeguard assets and guarantee the integrity of business processes. Based on this analysis, P&G will either take no further investigative action or will proceed with a proportional investigation using active monitoring tools.

P&G uses five basic types of Active Monitoring tools: (1) Device Scanning, (2) Internet Scanning, (3) Soft Monitoring, (4) Hardware Monitoring, and (5) Data Loss Prevention.

1. **Device Scanning:** These tools permit P&G, sometimes through a third-party, to pull the *entire* contents of a P&G owned computer or other P&G device at a single point in time for use in an investigation. Device Scanning tools not only pull the files and applications saved and stored on the P&G device, but can grab the memory present on the that device at the time of capture as well. Depending on the tool, P&G may choose to pull only physical files (i.e., no memory) or pull a partial image of the device – allowing the investigation to focus only upon specific file types or applications in accordance with the principles of proportionality.
2. **Internet Scanning:** P&G deploys a third-party cloud-based web proxy tool that has three primary features. First, it has the capability to track public internet usage at the URL level (i.e. the names of the webpages visited) when the EPR is using a P&G owned device. This

feature tracks and logs internet activity by using hashed personal identifiers (therefore de-identifying the user) for potential use in an approved investigation. Second, it has the capability to provide visibility into the data entered into an unencrypted webpage and the files uploaded or downloaded when visiting unencrypted websites. Third, it has the capability to decrypt a limited subset of web traffic that is predefined as high risk (e.g., outbound connections to known malicious webpages, webpages known to deliver malware to devices, or unapproved filesharing sites). This solution is configured to not decrypt traffic bound for websites that may process sensitive personal information about the end user (e.g., banking and healthcare sites).

3. **Soft Monitoring:** These are techniques deployed as part of an investigation involving identifiable individuals where (a) the individual is made aware of the investigation, and (b) the individual is not the subject of the investigation. For example, a Soft Monitoring tool might be a phone call or an email to determine where an *identified* EPR is currently located/logged-in to determine if a geographic triggered Event is legitimate.
4. **Hardware and Application Monitoring:** Hardware and Application Monitoring tools are logging and monitoring capabilities that the manufacturers build into the hardware and/or applications that, when combined with an identifiable EPR, constitute Active Monitoring. Commonly used examples are server logs, SAP logins, ID badge swipe reports, network authentication, etc.
5. **Data Loss Prevention:** P&G or an approved service provider scans emails bound for non-P&G addresses for indicators of data loss. For example, if an EPR sends an unencrypted email with a Highly Restricted attachment to a non-P&G email address, the data loss prevention solution would flag that email as an information security risk, and the user may be informed that they need to use an approved encryption solution for future communications. Similarly, if an outbound email classified as Highly Restricted or Secret (including specifically designated key words) were flagged, that email would then be reviewed for security risk. If appropriate, an investigation may be initiated. P&G does not scan messages that are classified as "Personal" or "Private" or that are marked as "Personal" or "Private" in the subject line.

6.0 Future Modifications

P&G reserves the right to modify this Notice as needed, for example, to comply with changes in laws, regulations, Company practices and procedures, or to respond to new threats or new requirements imposed by data protection authorities. Where such changes materially affect our processing of your EPR Personal Information, we will notify you accordingly.

7.0 Contact Information

If you have any questions, complaints or concerns with respect to our processing of your personal data/EPR Personal Information or if you wish to exercise your privacy rights, you may contact our Global Data Protection Officer at – Email: pgprivacyofficer.im@pg.com, Phone: +1 (513) 622-0103, Mailing Address: 1 Procter & Gamble Plaza, Cincinnati, OH 45202, U.S.A.

If you have concerns about a potential data breach of your EPR Personal Information or any personal information being handled by P&G, please email us at securityincident.im@pg.com.

California State Addendum

If you are a resident of California, this supplemental notice (“Addendum”) applies to the processing of EPR Personal Information and is provided to you in order to share certain information required by the California Consumer Privacy Act and the California Privacy Rights Act (collectively, the “CPRA”). This Addendum is provided in addition to the Global External Party Resources Privacy Notice (the “Global Policy”).

Capitalized terms not defined in this Addendum are defined in the Global Policy.

1. Sources of Personal Information

In many cases, P&G collects EPR Personal Information directly from you or from your employer. We may also obtain information about you from P&G service providers or P&G employees. We may collect information about you automatically when you use our computer systems, swipe your access badge, or visit sites where CCTV images are being recorded. In each case, we only collect those data types that are needed for P&G’s appropriate business purposes.

2. General Purposes for Collecting, Using and Disclosing Personal Information

P&G collects and uses EPR Personal Information for the purposes set forth in the Global Policy.

3. Specific Categories of Personal Information

P&G collects and uses the specific categories of EPR Personal Information as described in the Global Policy.

4. Sensitive Personal Information

Sensitive Personal Information for the purposes of this Addendum is defined by CPRA and includes the data types listed in the chart below. P&G collects, uses, and discloses Sensitive Personal Information as needed for the purposes set forth below and does not use or disclose Sensitive Personal Information about EPRs other than as necessary for our human resources and compliance functions and for other legally authorized purposes.

Category of Sensitive Personal Information	Purposes for Use and Disclosure
Government-issued Identification Numbers (including passport, visa, social security number, driver’s license, and other government-issued identifications)	As set forth in Global Policy
Account log-in credentials and financial account numbers (with password, access code or other credential that permits access to an account)	As set forth in Global Policy
Contents of Mail, Email or Text Messages	As set forth in the Global Policy
Biometric Identifiers	As set forth in the Global Policy
Health Information	As set forth in the Global Policy To note, P&G does not collect or use Genetic Data.

5. Collection of Personal Information by Third Parties

In most cases, P&G only allows third parties to control the collection of EPR Personal Information when those third parties are acting as a service provider or a contractor to us. These companies

only retain, use and disclose your personal information in accordance with our contracts and applicable laws. Please refer to the Global Policy for more information on how P&G uses cookies, such as Google Analytics.

6. Disclosures to Service Providers, Contractors, and Third Parties

P&G does not sell Personal Information pertaining to EPRs or share it with third parties for cross-contextual behavioral targeting. P&G may disclose EPR Personal Information as set forth in the Global Policy. For clarity as it relates to CPRA, the following circumstances may also apply:

- P&G may disclose EPR Personal Information with our service providers, contractors, and third parties. These companies may only use the data only as permitted by our contracts with them.
- We may share limited elements of EPR Personal Information with third parties as may be appropriate. For example, if you are an EPR in an external-facing role, we may share your name and business contact information as needed.

7. Your California Privacy Rights

P&G respects your privacy rights. When exercising these rights, we encourage you to first discuss your concerns with the P&G employee who serves as your site sponsor. EPRs may also exercise these rights by calling (833) 592-6929, or by clicking [here](#) and selecting the option for contractors.

The CPRA provides California residents with specific privacy rights:

- The right to know what Personal Information and Sensitive Personal Information we collect
- The right to access your Personal Information
- The right to correct inaccurate Personal Information
- The right to request that we delete your Personal Information
- The right to know what categories of Personal Information are sold to third parties and to opt-out of those sales
- The right to know what categories of Personal Information are shared with third parties for cross-contextual behavioral targeting and to opt-out that sharing
- The right to limit the use and disclosure of Sensitive Personal Information, and
- The right not to be retaliated against for exercising your privacy rights

To note, P&G does not sell Personal Information pertaining to EPRs or share it with third parties for cross-contextual behavioral targeting. Further, P&G will only process your Sensitive Personal Information as described in the Global Policy and this Addendum.

8. Data Retention

The retention periods for EPR Personal Information vary depending on the nature of the business records in which the data elements are maintained. The retention period for our business records are set based on the following criteria: (1) the length of time that the record is needed for the purposes for which it was created, (2) the time the record is needed for other operational purposes, such as audits and reporting, (3) the length of time the record is needed for legal compliance, including maintain of opt-out/in lists, legal defense and legal holds.

9. Questions or Complaints

Please refer to the Contact Information found in the Global Policy.