Ethics & Compliance Office

Global Employee Privacy Policy

Privacy Notice Contact:	corporateprivacy.im@pg.com	**Date:**	March 21, 2024
Region:	Global	**Scope:**	All Employees

1.0 Intent

P&G values the trust and loyalty of our Employees and has designed this Global Employee Privacy Policy ("Policy") to meet both the business needs of the Company and the security and protection of P&G Employees' Personal Information. This policy informs you of how The Procter & Gamble Company, its subsidiaries and/or affiliates ("P&G" or the "Company") will collect and manage Employee Personal Information. It also describes the Company's expectations for those who collect and manage Employees' Personal Information on the Company's behalf.

This Policy is in line with P&G's Purpose, Values, and Principles ("PVPs"). In addition, many countries have specific legal requirements governing the use of Personal Information, including Employee Personal Information. The Company will comply with all such laws and regulations, including local data protection and co-determination laws, and it will implement additional procedures, standards, and policies wherever needed to meet these requirements. Accordingly, the actual Employee Personal Information collected in a particular jurisdiction or that may be accessed by P&G in a particular jurisdiction may be unique to comply with local laws. In addition, this Policy will be supplemented by country-specific addenda where applicable.

2.0 Definitions

Employee: For the purposes of this policy, the term Employee includes current and former P&G employees and retirees.

Personal Information: Any information relating to an identified or identifiable individual.

Sensitive Personal Information: Personal Information revealing race, ethnicity, political views, religion, health, sexual orientation, trade union membership, genetic or biometric data, information about criminal convictions and offenses, and as otherwise defined by law.

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.

3.0 Principles

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

- Collect and manage the minimum amount of Employee Personal Information.
- Respect individual privacy.
- Comply with our PVPs, this Policy and relevant laws.
- Follow appropriate standards and procedures when collecting and/or managing Employee Personal Information.

4.0 Notice

P&G respects your privacy. This policy describes how we process Employee Personal Information, the types of information we collect, for what purposes we use it, with whom we share it, and the choices you can make about our use of Employee Personal Information. We also describe the measures we take to protect the security of Employee Personal Information and how you can contact us about our privacy practices.

4.1 For What Purposes Do We Collect and Use Employee Personal Information?

P&G collects Personal Information about its Employees in the context of the employment relationship and related HR processes. We generally collect and use Employee Personal Information for the following business processes, including, but not limited to the following services and/or activities:

- Compensation/payroll management, tax reporting salary planning, and company benchmarking
- Corporate credit card use, travel expense accounting and expense reimbursement
- Benefits management, including health insurance, retirement/pension benefits, and other voluntary benefits
- Relocation and travel management, including government-required travel documentation
- Time and attendance management, including vacation, disability leave, sick leave and other leaves or absences
- Staffing, performance management, career development, trainings and recognition
- Occupational health/safety and wellness programs
- Health-related screenings and medical programs related to COVID-19 or similar health crises
- Site access management, facilities support, and security and contingency planning purposes
- Electronic device enrollment and management, and network and device usage optimization
- Physical and cyber security controls, including electronic device and network monitoring
- Facilitating the sale or transfer of assets including the totality or part of the Company or its businesses
- Litigation and internal/external investigations, audits, and dispute resolution
- Perform enterprise data analytics leveraging data contained in P&G's human resources and related systems of record (e.g., Workday, SAP, Workforce Management, etc.). This processing enables Human Resources, specialized analytics teams, and organizational leaders to obtain aggregated data-driven insights to understand the state of the organization, improve workforce planning, develop human resources management and talent planning processes to design a healthy organization positioned to succeed and to offer its employees best work environment. Examples of such types of analytics include: attrition analyses, hiring forecasts,

analyses to assess employee satisfaction, equal opportunities areas of improvement, talent pipeline, employee learning and development, salary benchmarking, analyses related to time and workforce management, etc. Analysis are conducted only by authorized personnel following specific guidelines in order to protect privacy and confidentiality of your data. P&G analyzes and aggregates the data and these analytics are not used for individual profiling or decision making. The primary lawful basis for these analytics activities is legitimate interest.

- Daily work processing (e.g., authenticating and logging into our systems)
- Corporate meetings and events, and training and employee communications
- Delivery of gifts and other Company materials and products to employee households
- Diversity, equality and inclusion efforts (e.g., designing, staffing and promoting a diverse and inclusive organization and workplace)
- Facilitating trade union membership
- Facilitating affinity group membership
- Other personnel related data management, including employee care, IT and human resources support
- Compliance with banking, due diligence, and know-your-client (KYC) requirements from our financial partners (e.g., for opening and managing corporate bank or financial accounts)
- Facilitating tax and other governmental incentives
- Compliance with laws, regulations and Company policies regarding antibribery, child labor, anticorruption, sanctions, export controls, human rights and other corporate governance and stewardship requirements
- Compliance with all legal, regulatory, judicial or governmental requirements
- Facilitating charitable contributions to corporate campaigns or local volunteer efforts

Whenever reasonably possible and consistent with P&G's legitimate business interests, your consent, the Company's legal obligations, and/or to comply with the Company's contractual obligations, P&G will inform you about the Personal Information that is collected about you and how it will be used.

4.2 What Types of Employee Personal Information Do We Collect?

We collect and manage the minimum amount of Employee Personal Information needed to comply with our contractual and/or legal obligations as an employer; to support the Company's legitimate business interests in a way that is proportional to the privacy interests of its Employees; and to process personal data provided with your consent, when applicable, for its intended purposes.

The below chart describes in more detail the categories of Employee Personal Information that P&G collects in connection with its employment and human resources processes. Each category of Personal Information listed below also may be used as described in Section 4.1 above.

Note that we will always minimize the types and amount of Employee Personal Information the Company may collect from or about you. 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 Employee Personal Information will vary by data type and intended use, as described in Section 4.3 below.

Which Types of Employee Data Do We Collect and Process?	**Why Do We Collect and Process Different Types of Employee Personal Information?** ***We collect and process these data types for multiple organizational and business processes as detailed in Section 4.1, and as further explained below:***
Contact Information and Personal Characteristics • Full name or previous names (such as maiden names) • Gender, including pronouns • Date and place of birth • Marital status • Family/household composition • Honorifics and titles, including preferred name and salutation • Physical/mailing address • Email address • Telephone number • Mobile number	• Human resources records and business processes • Organizational charts and directories • Compensation and payroll management • Benefits management • Occupational health and wellness programs • Corporate travel logistics and security • Staffing and organizational planning • Training • Site and electronic network access • Communications with you about your employment, including sending you work schedule information, compensation and other Company information • Legal and policy compliance; corporate governance and stewardship; security and contingency planning; required external reporting; investigations and incident management • Facilitating charitable contributions to corporate campaigns or local volunteer efforts
Government ID/Work Eligibility Information • National ID (such as passport, visas, social security number, driver's license, other government-issued identifications) • Citizenship	• Legally identifying you and maintaining the integrity of our human resources records • Complying with immigration and other work permit requirements

• Residency • Nationality • Country of birth • Military and/or veteran status	• Security and risk management, such as collecting driver's license data for employees who operate Company automobiles, professional license verification, fraud prevention and similar purposes • Designating representatives in legal, government or regulatory proceedings • Designating P&G employees as representatives and/or authorized signatories for representing the Company (including managing banking and financial accounts) • Obtaining tax and other government incentives benefiting our employees and/or operations • Legal and policy compliance; corporate governance and stewardship; security and contingency planning; required external reporting; investigations and incident management
Professional Data • Information collected during or after the employment application process, including academic data, professional licenses, certifications, memberships and affiliations • Company employee ID number • Personal and professional skills (e.g., languages spoken), interests and hobbies • P&G dates of employment • P&G positions held, including band level and title • P&G work locations, including physical and mailing addresses • P&G email and phone numbers • P&G performance, attendance, disciplinary and grievance records and reviews • Training plan records • Data from LinkedIn profiles and similar professional platforms • Professional goals and interests • Information provided for Company social and professional industry associations • Trade union membership	• Human resources records and business processes • Organizational charts and directories • Staffing, organizational design and business continuity purposes • Supporting our employees' career progression, as well as their professional and personal goals • Promoting equality and inclusion in the workplace • Designating P&G employees as representatives with external business partners including banks and financial institutions • Determining and verifying appropriate authority to review or approve business processes (e.g., band level) in compliance with applicable Company policies. • Legal and policy compliance; corporate governance and stewardship; security and contingency planning; required

	external reporting; investigations and incident management
Financial information • Bank account number and details • Company-issued payment card information, including transaction records • Personal payment card information, if provided for reimbursement	• Facilitating payroll processes, benefits management, relocation expenses, and travel and expense reimbursement • Legal and policy compliance; corporate governance and stewardship; security and contingency planning; required external reporting; investigations and incident management
Health Information • Information related to the physical or emotional health of an individual, including any disabilities or limitations to perform work duties or functions • Genetic data (strictly for certain legally required occupational health exams, when genetic data may influence the results of such health exam) • Drug testing and other types of health examinations	• Determining your fitness to work in a particular role, and reasonably accommodating any disabilities • Supporting your ability to participate in our leave of absence and/or disability insurance programs • Complying with occupational health and workplace safety and government reporting requirements • Managing employee safety and business risks associated with the COVID-19 pandemic, or similar health emergencies • Facilitating your participation in health benefit programs, including our health plans and Vibrant Living programs; and • Legal and policy compliance; corporate governance and stewardship; security and contingency planning; required external reporting; investigations and incident management
Electronic Identification Data/ Unique Identifiers / Image & Voice	

• P&G system identifiers (e.g., usernames or online credentials) • Digital signature • Electronic identification data, logs and records regarding your access and use of P&G devices, the P&G network (such as your use of email, the internet, social media), P&G systems, applications, licenses and any other P&G database • 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 your access to P&G sites and access-restricted areas, including badge number/badge identifier 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 • Evaluating compliance with Company policies related to use of our electronic network and devices, including but not limited to hardware and software • Evaluating compliance with Company policies regarding physical and cyber security • Internal record-keeping and reporting, including data matching and analytics • Enabling your access to P&G sites, network, tools, applications and other Company systems and assets • Drive visibility on the use and costs for consumption of P&G tools, licenses, services and applications for optimization, quality, audit and cost purposes • Memorialize trainings and meetings • Legal and policy compliance; corporate governance and stewardship; security and contingency planning; required external reporting; investigations and incident management
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. 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 as a person. Cookies show your computer and device only as randomly assigned numbers	We use cookies in P&G Employee-facing websites for a number of reasons, such as: ▪ to learn more about the way you interact with our websites and P&G content

and letters (e.g., cookie ID ABC12345) and never as, for example, John E. Smith. These are the types of cookies we use: ▪ *Session Cookies*. Webpages have no memory. Session cookies remember you (using a randomly generated ID like ABC12345) as you move from page to page so that you don't get asked to provide the same information you've already given on the site. These cookies are deleted as soon as you leave our site or close your browser. ▪ *Persistent Cookies*. 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. Not having to select a language preference every time makes it more convenient, more efficient, and user-friendly for you. ▪ *Analytics Cookies*. 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. 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.	▪ 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 ▪ Legal and policy compliance; corporate governance and stewardship; security and contingency planning; required external reporting; investigations and incident management
Children's data/Family Composition • Child's name, date of birth and relationship to the employee • Contact Information and Personal Characteristics of employee dependents, family members and/or household members	• Benefits' enrollment and dependent verification • Supporting logistics related to international assignments and relocation • Complying with immigration and customs requirements related to travel and relocation • Supporting employee and business continuity in the event of crises • Facilitating Company activities involving dependent, family and/or household members; and • Legal and policy compliance; corporate governance and

	stewardship; security and contingency planning; required external reporting; investigations and incident management
Other Personal Characteristics • Ethnicity • Race • Sexual orientation & gender identity • Disabilities • Political views • Religious/philosophical beliefs • Biometric data, such as fingerprints or facial scans • Criminal history	• Supporting equality and inclusion programs that promote a diverse workplace, including related human resources analytics • Facilitate your participation in Company affinity programs • Facilitating your access to Company sites and systems via biometric data • Supporting talent planning activities, recruiting, staffing and careers • Legal and policy compliance; corporate governance and stewardship; security and contingency planning; required external reporting; investigations and incident management

4.3 Under What Legal and/or Business Basis Do We Process Employee Personal Information?

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

The legal and/or business basis for processing Employee Personal Information may vary by jurisdiction, as well as by the data category/type and the reasons why we collect and use such information. Where required by law, we fully document the specific legal and/or business basis for processing Employee Personal Information before collecting and using such data.

These are some examples of the legal/business basis for processing certain Employee Personal Information:

Type of Personal Data	Purpose of Processing	Legal/Business Basis for Processing
Government ID, Financial Information	Supporting payroll and tax reporting activities	P&G's compliance with contractual and legal obligations arising out of the employer-employee relationship

Race, Ethnicity, Sexual Orientation	Facilitating your participation in Company-sponsored Affinity Groups	Your consent
Nationality, Citizenship	Complying with immigration and other work permit requirements	P&G's compliance with applicable laws and regulations
Professional Data	Staffing, organizational design and business continuity purposes	P&G's legitimate business interests

4.4 How Do We Share Employee Personal Information?

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

P&G may share your information with contractors, suppliers, agencies, temporary workers, or any other parties acting on P&G's behalf ("External Parties") who perform P&G business operations on our behalf. The Company requires that External Parties provide equivalent levels of protection as applied by the Company when handling Employee Personal Information. We contractually require External Parties operating as data processors to only process the data in accordance with our instructions and to secure the data. These data processors may not otherwise use or disclose the information, except as authorized by P&G, and/or to comply with legal requirements.

There are certain situations where P&G will share or you will be asked to share personal information directly with providers connected to P&G's employee services or benefits which act as Data Controllers and thus are directly responsible for protecting your Personal Data and P&G does not control how your data is processed (e.g., pension, healthcare, financial and or benefits providers). If you enroll in our benefits programs, we may disclose your personal information those companies that provide the benefits and services to you. These companies will provide you with their own privacy statements. In those situations, please ensure you read and understand the privacy policies and practices of such providers.

Employee Personal Information may be shared with our headquarters and affiliates globally as necessary to fulfill business-related purposes. You can find information on how we protect Employee Personal Information in such a situation in Section 4.6 of this Policy.

We may also disclose Employee 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; to assist in the investigation of suspected or actual misconduct or illegal activity; and/or as part of a sale of a P&G business to another company.

4.5 What Are Your Privacy Rights?

You have the right to contact us and request to access the Employee Personal Information that we process and use about you. You may request that inaccurate, outdated or no longer necessary information be corrected, erased, or restricted. Where required by applicable law, you may 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 Employee Personal Information is based on consent, you have the right to withdraw your consent at any time. Where the processing of

Employee 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 visit Workday (https://workday.pg.com/) - login with your P&G credentials) and review the "Personal" section within your Profile to verify your Employee Personal Information, update it and download it as needed (Update Personal Information job aid). For any additional requests, please contact Employee Care at GetHelp.pg.com or a Human Resources representative in your country. If you are not happy with our response to your requests, you may lodge a complaint with the data protection authority in your country.

4.6 How Do We Transfer Employee Personal Information?

If legally allowed, and subject to country requirements and/or limitations, Employee Personal Information may be transferred to other countries. P&G is a global business and has Employees in many countries. Employee 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 of the world as necessary to conduct the relevant operations, in compliance with applicable law. This means that your Employee Personal Information may be transferred to countries outside the country in which you work. Those countries may not have the same data protection laws as your country of residence. When your 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 information. We perform transfers outside of the European Union, both among P&G entities and between P&G and our service providers, using contractual protections that EU regulators have pre-approved to ensure your data is protected (known as Standard Contractual Clauses). If you would like a copy of a transfer agreement, contact corporateprivacy.im@pg.com. P&G will also comply with other specific country requirements that restrict data transfers outside of the country of collection, require contractual provisions regarding the transfer, and/or that require data localization.

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: Worker Privacy Policy*.

4.7 How Do We Secure Employee Personal Information?

We implement appropriate physical, administrative, and technical measures, such as pseudonymization, encryption and access controls, designed to protect Employee 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 Employee 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.

4.8 How Long Do You Keep my Personal Information?

We keep Employee Personal Information for as long as necessary to fulfill business-related purposes unless a longer retention period is required or permitted by applicable law. In some cases, we may need to retain Employee 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.

4.9 Does P&G Monitor Network and Device Usage?

The Company monitors some network and device usage. P&G has an obligation to protect its employees, assets, and facilities. To that end, P&G has created an Electronic Network and Device Monitoring Policy to help meet our legal obligations and to help employees understand how this monitoring activity protects them and the Company. You can access this policy via privacy.pg.com or request a copy via corporateprivacy.im@pg.com. Under this policy, P&G monitors its 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. This monitoring is consistently handled in compliance with relevant laws and Company policies.

5.0 Sensitive Categories of Personal Information and "SPI" on P&G Networks and Devices

P&G acknowledges that certain types of data are more sensitive than others. Privacy laws around the world often use differing terminology in naming these categories of sensitive data and also set varied compliance requirements for companies to follow in their processing of this data. No matter the terminology and requirements set by local laws, P&G ensures that it meets the relevant compliance elements in its processing of these more sensitive categories of personal data. In addition, P&G has, for purposes of some countries' laws, labelled some categories of higher sensitivity data as "Sensitive Personal Information" or "SPI." P&G defines SPI to be any information relating to an identifiable person that includes or implies race, ethnicity, political views, religion, health, sexual orientation, genetic or biometric data, and information about criminal convictions and offenses.

To limit P&G's potential to access your Sensitive Personal Information in the course of running its business operations, your **personal use of SPI is prohibited on P&G networks and devices**. This means that an employee may not use Company devices (e.g., computers, Company-provisioned tablets, CorporateMobile, etc.) or Company networks (P&G wireless internet connections, telephony networks, and LAN) for personal purposes involving SPI. For example, employees should not visit websites that strongly imply SPI such as medical specialists' webpages or webpages for houses of worship. This means that employees may NOT use functionality like email/calendar/web browsing for any *personal* activity that uses or implies SPI data. To be clear, P&G will not monitor SPI (or any data for that matter) on personal employee devices that do not connect to P&G networks.

Related to the previous paragraph, the only permitted use of SPI is *Company-related*. For Company-related purposes, P&G processes and uses your SPI in only in two, specific ways: (1) as required for business and employment purposes (e.g., providing you with health benefits, recording work disabilities or injuries, etc.) and (2) based on your consent when you participate in Company-approved groups (as examples, GABLE and AALN), use Company-sponsored applications that might gather SPI (for example, a Company health and wellness app) or provide it voluntarily for purposes of self-expression and enable P&G to design and staff a diverse and inclusive organization.

Given the above, P&G will only process Sensitive Personal Information to provide you with a Company benefit, fulfill an obligation under employment law, design, and staff a diverse and inclusive organization and/or to protect your data from cybersecurity threats. If you have more questions about what SPI is and/or how P&G handles such data, please contact the corporate privacy team, at this email address: corporateprivacy.im@pg.com.

6.0 Abiding by this Policy

Employee Personal Information should only be handled by individuals who have been authorized to do so by the Company. All such individuals must abide by this Policy.

As noted above in Section 4.4, the Company expects its Employees and any External Parties who collect or manage Employee Personal Information to follow this Policy, whether they are utilizing P&G's and/or their own electronic systems and data management tools. Employees are also responsible for ensuring that any External Parties they work with in support of P&G operations comply with this Policy.

Failure by Employees to comply with this Policy can result in disciplinary action which may include termination. All disciplinary action will be applied in a manner consistent with local law. For External Parties collecting or managing Employee Personal Information on P&G's behalf, failure to comply with this Policy can lead to negative business consequences, up to and including termination of the business relationship, referrals to regulatory authorities, and/or claims for damages.

The Company makes every reasonable effort to ensure that Employee Personal Information is accurate and up to date for its intended use. Employees are also responsible for updating and checking the accuracy of the information provided to P&G. If you provide Personal Information of others (e.g., of your beneficiaries and family members), you have the obligation to ensure the lawfulness of your provision of this Personal Information to the Company. Employees are also responsible for protecting the privacy and security of their and other employees' Personal Information by complying with the Company's information security guidelines and policies, which can be reviewed at http://security.pg.com

Each P&G business unit shall perform its own self-assessments of compliance with this Policy. In addition, P&G Global Internal Audit will periodically assess whether Employees and relevant External Parties comply with this Policy and related Company standards and procedures when they handle Employee Personal Information. Appropriate follow-up measures, if necessary, are enforced.

7.0 Future Modifications

P&G reserves the right to modify this Policy 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 Employee Personal Information, we will accordingly notify you.

8.0 Contact Information

The P&G entity with which you have your employment relationship is your employer and therefore the controller of your Employee Personal Information. If you want to learn more about the Employee Personal Information we collect and how we use it, contact your relevant HR representative or email

us at corporateprivacy.im@pg.com. If you have these or any other questions or concerns with respect to our processing of your personal data/Employee Personal Information, you may also 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.

Please also see Section 4.5 above for information about how to exercise any of your rights under applicable data protection laws. For contact information specific to certain countries, see Addendum A to this Policy. If you have concerns about a potential data breach of your Employee Personal Information or any personal information being handled by P&G, please email us at securityincident.im@pg.com.

9.0 Additional Information

Resources: Resources available to you are listed on Privacy Central: privacy.pg.com

Questions About Use of Your Employee Personal Information: If you are asked to provide Personal Information about yourself or your family members and you question the business relevancy of the request or if you have other questions or concerns regarding your Employee Personal Information, please contact your HR representative.

Reporting Potential Policy Violations: If you feel this Policy has been violated, you have many resources available to help you, including your immediate manager, your HR representative, the Company's Global Data Protection Officer, a member of the P&G Legal Division, the WBCM Helpline (where applicable) or send an email to corporateprivacy.im@pg.com. We will follow the Company's Incident Response Guidelines for any reported violation.

ADDENDUM A

Asia:

Procter & Gamble Philippines, Inc.
Jocelyn J. Gregorio-Reyes
gregorioreyes.j@pg.com
+632558-4250

Procter & Gamble International Operations SA (ROHQ) – GBS
Jennifer Pascual-Sy
pascualsy.jl@pg.com

Procter & Gamble Korea S&D Company
Lincoln Park

park.lc@pg.com
+82-2-6940-6361

European Union:

Belgian Pension Fund
Guido Pieroth
pieroth.g@pg.com
+41-58 004 7560