

This document is in two parts: Privacy Guidelines and Security Guidelines. Please read both thoroughly.

PRIVACY GUIDELINES

P&G's privacy guidelines and practices are consistent with The European Union Data Protection Directive through the U.S. Department of Commerce Safe Harbor Program, Fair information practices established by the Organization for Economic Co-operation and Development (OECD), The Asia Pacific Economic Cooperation forum (APEC) Privacy Framework, applicable national and state data protection laws and the American and Canadian Institutes of Certified Public Accountants Generally Accepted Privacy Principles.

These privacy guidelines apply to vendors who collect, use, transfer or store personal information.

Simply put, P&G's privacy goal is to protect, collect, and use personal information provided to us as they would expect.

- We use personal information only for purposes consistent with the reason it was provided.
- We do not share personal information with other marketers.
- Our privacy policy applies to:
 - All individuals who provide personal information such as consumers, customers, research subjects, business partners, shareholders, job applicants, employees, retirees, and others.
 - All locations where we operate, even where local regulations do not exist.
 - All methods of contact such the internet, direct mail, telephone, mobile, and for emerging technologies and methods that might be tested.

Consult the Privacy Central Website for the current executional requirements and examples of approved wording. (Access is via <https://privacy.pg.com>, contact the P&G Purchases spend pool owner for ID/Password)

1 Benefits for individuals:

- 1.1 Minimum necessary: Collection of personal information should be limited to the minimum amount of information necessary to meet the needs of the program; do not collect information that is not needed.
- 1.2 Plan for Use: Collection of personal information should be limited to what is planned for use within a reasonable time period. Do not collect information if there is no plan in place to use the information. This is necessary to reduce the likelihood of future contact being perceived as SPAM or a non-value added communication to the individual.
- 1.3 Collected purpose only: Personal information is to be used only for the purpose that was specified at the time of collection.
- 1.4 Not shared: Information that is collected for P&G programs cannot be shared with other marketers or agents.

2 Notice:

- 2.1 Notice at collection: A privacy notice should be provided for all channels when collecting personal information. This notice should tell individuals what information we collect, how it is used, whether it may be temporarily transferred to others to provide the products or services requested, if it will be transferred outside the country of origin, and how to contact P&G with privacy questions.
- 2.2 Notice at Use: A privacy notice should be provided whenever an individual is contacted.
- 2.3 Acceptable Notice: Appropriate Privacy notices are provided on Privacy Central. Obtain Corporate Privacy Office permission for proposed variances from current approaches listed on Privacy Central.

3 Choice:

- 3.1 Affirmative consent: P&G is an Opt-in company. Obtain affirmative opt-in to contact the individual in the future. Do not contact individuals where we do not have affirmative consent.
- 3.2 Clear and Obvious: Consent should be requested via obvious, clear and simple language provided at the time / place of opting in, so the individual is fully aware of what they are opting into and how their information will be used. Do not place this consent with other pages such as in Terms and Conditions.
- 3.3 Consent based contact: Contact only individuals who have asked to be contacted. For example, use purchased lists of names only from providers who verify that consumers have consented to hearing from companies such as P&G.

- 3.4 Co-marketing arrangements: Obtain Corporate Privacy Office guidance for all co-marketing efforts (where consumers may be opting in to both P&G's and another party's program) to ensure appropriate notice and choice have been provided.
- 3.5 Opt out provisions: Provide an "opt-out" option whenever contacting an individual for ongoing purposes. This opt out is required for all channels.
- 3.6 Processes for opts: Verify that back-end processes are in place to process the opts that are collected.
- 3.7 Suppression lists: "Scrub" all outbound communication against appropriate suppression lists, from external organizations, such as the DMA as well as internal P&G lists.
- 3.8 Current best approach: Consult Privacy Central for guidelines, current approaches and appropriate wording. Obtain Corporate Privacy Office permission for proposed variances from current approaches listed on Privacy Central.

4 Technology:

- 4.1 Privacy impacting technologies: Tell individuals if technologies are used that are privacy related; for example telephone caller ID. Do not use technologies that the individual may not be aware of to collect personal information.
- 4.2 No information on individual's computer: Cookies, files or other technologies stored on an individual computer by P&G programs must never contain personal information.
- 4.3 New technologies: Obtain permission from the Corporate Privacy Office when utilizing any new technology to collect personal information, store personal information, or track personal information to verify that it is consistent with P&G Privacy Policy.

5 Data Accuracy & Access:

- 5.1 Correct information: Take appropriate steps to make sure that the personal information used is correct.
- 5.2 Correct lists: Use good lists; make sure that purchased lists use valid data, both the personal information and the demographics connected with that information.
- 5.3 Data hygiene: Verify that the list hygiene or name merging used does not merge one individual's information with another's.
- 5.4 Access to information: Ensure a process is in place to provide individuals reasonable access to their personal information.
- 5.5 Update to information: Ensure a process is in place for individuals to update and correct their personal information.
- 5.6 Online access: Use two factor authentication when providing access online.

6 Security:

- 6.1 P&G security guidelines: Follow the P&G security requirements section in this document for vendors to protect personal information by industry standard security practices and measures, in order to prevent loss, misuse, unauthorized access, disclosure, or alteration.
- 6.2 Control access: Limit access to personal information to those who have a business need.
- 6.3 Data retention: Delete data when it is no longer needed; do not keep personal information any longer than necessary to meet the business need.

7 Data / File Transfer

- 7.1 Cross border transfer: Verify that the correct data transfer contracts are in place prior to transferring the information, if personal information is to be transferred to any country other than the country where is collected.
- 7.2 Sensitive information: Use industry standard 128 bit encryption (SSL) when collecting and transferring sensitive information including personal information from US P&G Health care sites.
- 7.3 File transfer: Use secure file transfer protocols when transferring data files.
- 7.4 File receipt: Limit the number of people that data files are sent to

8 Children:

- 8.1 Do not collect: Do not collect personal information online from individuals under the age of 13.
- 8.2 Age check online: Verify that websites and other online programs only collect information from individuals over the age of 13 by asking for birth date before collecting personal information. This includes mobile programs that provide opt in via online processes. Consult Privacy Central for guidelines, and appropriate wording for age checking.
- 8.3 Approval to collect: Obtain consent from the P&G country legal representative prior to collecting information from children for programs executed in countries other than the US. Obtain approval from

the P&G Corporate Privacy Office to collect personal information from children under the age of 13 for all programs other than the Beinggirl program

8.4 Minimal collection: Ask only for the minimum information necessary from a child to participate in the program.

8.5 Parental access: Implement a process where parents can obtain a copy of the information their child has provided, or update the information, or to ask us to no longer use the information when collecting information from children.

9 Accountability:

9.1 Management Commitment: Establish and demonstrate top management's commitment to maintaining the trust placed in P&G by those who give us personal information by following P&G Privacy guidelines and implementing appropriate privacy and security.

9.2 Privacy Responsibility: Appoint an individual to coordinate the information privacy arrangements in business units/departments. This individual should have enterprise-wide responsibility for verifying that P&G's information privacy requirements are implemented.

9.3 Privacy Training and awareness: Employees should be made aware of the key elements of P&G's privacy requirements and understand their personal responsibilities. Staff should be educated/trained in how implement P&G's privacy requirements.

9.4 Executorial accountability: Procedures should be in place to confirm that P&G programs are compliant with privacy before they go into production. Monitor programs and systems to ensure that personal information is secure, protected and used appropriately.

9.5 Privacy Incidents: Implement a program to be made aware of a privacy incident with P&G programs, and a process to notify the appropriate P&G person immediately if an incident occurs.

SECURITY GUIDELINES

P&G's security methodology is based the International Security Forum's (ISF) Standard of Good Practice, control areas from the ISF's FIRM methodology (both 1998 and 2005) and are consistent with the ISO/IEC 17799 Code of Practice for Information Security Management (both 2000 and 2005) and to the Control Objectives in ISACA's Control Objectives for Information and related Technology.

These security guidelines apply to vendors who collect, use, transfer or store personal information.

The guidelines described below are comprehensive in nature, and each vendor should develop a security program, containing administrative, technical, and physical safeguards and guidelines *appropriate to the size and complexity, the nature and scope of the activities, and the sensitivity of any individual information at issue.*

The security program must be reasonably designed to achieve the objectives to:

- (1) Insure the security and confidentiality of individuals' information;
- (2) Protect against any anticipated threats or hazards to the security or integrity of such information;
- (3) Protect against unauthorized access to or use of such information.

1 Information Security Governance

- 1.1 Management Commitment: Top management's direction on information security should be established, and commitment demonstrated.
- 1.2 Information Security Function: An information security function should be established, which has enterprise-wide responsibility for promoting information security.
- 1.3 Local Security Co-ordination: An individual should be appointed to co-ordinate the information security arrangements in business units/departments.
- 1.4 Security Audit / Review: The information security status should be subject to thorough, independent and regular security audits/reviews.
- 1.5 Security Monitoring: The information security condition of the enterprise should be monitored periodically and reported to top management.

2 Information Security Policy

- 2.1 Security Policy: A comprehensive, documented information security policy should be produced and communicated to all individuals with access to the enterprise's information and systems.
- 2.2 Security Architecture: An 'information security architecture' should be established, which provides a framework for the application of standard security controls throughout the enterprise.

3 Security Education / Awareness

- 3.1 Security Awareness: Employees should be made aware of the key elements of information security, why it is needed, and understand their personal information security responsibilities. Specific activities should be undertaken, such as a security awareness program, to promote security awareness to all individuals who have access to the information and systems of the enterprise.
- 3.2 Security Education: Staff should be educated/trained in how to run systems correctly and how to develop and apply security controls.

4 Accountability / Ownership

- 4.1 Staff Agreements: Staff agreements should be established that specify information security responsibilities, are incorporated into staff contracts and are taken into account when screening applicants for employment.
- 4.2 Roles and Responsibilities: An individual with overall responsibility for the development activity, together with business owners, should be appointed to manage system development activities, and responsibilities for key tasks assigned to individuals who are capable of performing them.

5 Information Risk Analysis

- 5.1 Risk Analysis: Critical applications, computer installations, networks and systems should be subject to a formal risk analysis on a periodic basis, the results of which should be documented, reviewed, and agreed by the appropriate owner.
- 5.2 Confidentiality Requirements: The impact of business information stored in or processed by the application being disclosed to unauthorized individuals should be assessed.

- 5.3 Integrity Requirements: The impact of business information stored in or processed by the application being accidentally corrupted or deliberately manipulated should be assessed.
- 5.4 Availability Requirements: The impact of business information stored in or processed by the application being unavailable for any length of time should be assessed.

6 Asset Management

- 6.1 Security Classification: The application, computer installation and network should be classified according to the criticality and sensitivity of information stored in or processed, using a security classification scheme that applies throughout the enterprise.
- 6.2 Asset Management: Proven, reliable and approved hardware/software should be used that meet security requirements and essential information about hardware and software (e.g. unique identifiers, version numbers and physical locations) are recorded in an inventory.
- 6.3 Handling Information: Additional protection is provided for handling sensitive material or transferring sensitive information. Files containing personal information are transferred via secure file transfer protocols. Sensitive information is encrypted.
- 6.4 Acquisition: Robust, reliable hardware and software should be acquired following consideration of security requirements and identification of any security deficiencies.

7 Identity and Access Management

- 7.1 Access Control: Access to the application and associated information should be restricted to authorized individuals and enforced accordingly.
- 7.2 User Authorization: All users of the computer installation should be authorized before they are granted access privileges.
- 7.3 User Authentication: All users should be authenticated by using UserIDs and passwords or by strong authentication mechanisms (e.g. smartcards or biometric devices, such as fingerprint recognition) before they can gain access to target systems.
- 7.4 Sign-on Process: Users should follow a rigorous system sign-on process before they can gain access to target systems.

8 Application and Services Security

- 8.1 Resilience: The applications, computer installations and networks should be run on robust, reliable hardware and software, supported by alternative or duplicate facilities.
- 8.2 Back-up: Back-ups of essential information and software should be taken on a regular basis, according to a defined cycle.
- 8.3 Web-enabled Applications: Specialized technical controls should be applied to web-enabled applications to ensure that the increased risks associated with web-enabled applications are minimised.
- 8.4 Ecommerce: A process should be established to ensure that information security is incorporated into electronic commerce initiatives enterprise-wide.
- 8.5 General Security Controls: The full range of general security controls should be considered when designing systems and services.
- 8.6 Application Controls: The full range of application and systems controls should be considered, and required controls identified.

9 Physical and Environmental Security

- 9.1 Physical Protection: All buildings throughout the enterprise that house critical IT facilities (e.g. data centers, network facilities and key user areas) should be physically protected against accident or attack.
- 9.2 Hazard Protection: Computer equipment and facilities should be protected against fire, flood, environmental and other natural hazards.

10 System Configuration

- 10.1 Host System Configuration: Host systems should be configured to function as required, and to prevent unauthorized or incorrect updates.
- 10.2 Workstation Configuration: Workstations connected to systems within the computer installation should be purchased from a list of approved suppliers, tested prior to use, supported by maintenance arrangements and protected by physical controls.
- 10.3 Configuration of Network Devices: Network devices should be configured to function as required, and to prevent unauthorized or incorrect updates.

- 10.4 Remote Working: Personal computers used by staff working in remote locations should be purchased from a list of approved suppliers, tested prior to use, supported by maintenance arrangements and protected by physical controls.

11 System Monitoring

- 11.1 Event Logging: Logs of all key events within the computer installation should be maintained (preferably using automated tools), reviewed periodically and protected against unauthorized change.
- 11.2 System Network Monitoring: Systems associated with the computer installation should be monitored continuously, and from a business user's perspective.
- 11.3 Intrusion Detection: Intrusion detection mechanisms should be applied to critical systems and networks.

12 Network Security

- 12.1 Installation and Network Design: Systems are designed with sufficient capacity to cope with predicted information processing requirements. Systems are protected by using a range of in-built security controls.
- 12.2 Network Documentation: Networks should be supported by accurate, up-to-date documentation.
- 12.3 External Access / Connections: All external connections to the network should be individually identified, verified, recorded, and approved by the network owner.
- 12.4 Firewalls: Network traffic should be routed through a firewall, prior to being allowed access to the network.
- 12.5 Wireless Access: Wireless access should be authorized, authenticated, encrypted and permitted only from approved locations.

13 Electronic Communication

- 13.1 Special Voice Network Controls: Voice network facilities (e.g. telephone exchanges) should be monitored regularly and access to them restricted.
- 13.2 Email: E-mail systems should be protected by a combination of policy, awareness, procedural and technical security controls.
- 13.3 Instant Messaging: Instant Messaging systems should be protected by a combination of policy, awareness, procedural and technical security controls.

14 Cryptography

- 14.1 Cryptography: Cryptographic solutions should be approved, documented and applied enterprise-wide.
- 14.2 Public Key Infrastructure: Where a public key infrastructure (PKI) is used, it should be protected by hardening the underlying operating system(s) and restricting access to Certification Authorities.

15 Information Privacy

- 15.1 Information Privacy: Responsibility for managing information privacy should be established and security controls for handling personally identifiable information applied.
- 15.2 Alignment with P&G Privacy: Personally Identifiable Information is collected, used, stored, transferred, and destroyed according to P&G privacy guidelines. Refer to the P&G Privacy Requirements for vendors section for details on use and collection of personal information

16 Malware Protection

- 16.1 Virus Protection: Virus protection arrangements should be established, and maintained enterprise-wide.
- 16.2 Malicious Code Protection: Enterprise-wide arrangements should be established to protect against malicious code, such as that downloaded from the web.

17 System Development

- 17.1 Development Methodologies and Environment: Development activities should be carried out in accordance with a documented system development methodology. System development activities should be performed in specialized development environments, isolated from the live environment, and protected against disruption and disclosure of information.
- 17.2 Quality Assurance: Quality assurance of key security activities should be performed during the development lifecycle.
- 17.3 Specification of Requirements: Business requirements (including those for information security) should be documented and agreed before detailed design commences.
- 17.4 System Design / Build: Information security requirements for the system under development should be considered when designing the system. System build activities (including coding and package customization) should be carried out in accordance with industry good practice, performed by individuals

provided with adequate skills/tools and inspected to identify unauthorized modifications or changes which may compromise security controls.

- 17.5 Testing: All elements of a system (i.e. application software packages, system software, hardware and services) should be tested before the system is promoted to the live environment.
- 17.6 System Promotion Criteria: Rigorous criteria should be met before new systems are promoted into the live environment.
- 17.7 Installation Process: New systems should be installed in the live environment in accordance with a documented installation process.
- 17.8 Post-implementation Review: Post-implementation reviews should be conducted for all new systems.

18 Change Management

- 18.1 Emergency Fixes: Emergency fixes to computer equipment, business applications, systems software and business information should be tested, reviewed and applied in accordance with documented standards/procedures
- 18.2 Change Management: Changes to any part of the computer installation should be tested, reviewed and applied using a change management process.
- 18.3 Patch Management: There is a strategy for patch management and a documented patch management process.
- 18.4 Remote Maintenance: Remote maintenance of the network should be restricted to authorized individuals, confined to individual sessions, and subject to review.

19 Incident Management

- 19.1 Incident Management: All incidents – of any type – should be recorded, reviewed and resolved using an incident management process.
- 19.2 Alignment with P&G Privacy: Incidents are reported to P&G immediately.
- 19.3 Forensic Investigations: A process should be established for dealing with incidents that require forensic investigation.

20 Third Party Management

- 20.1 Service Providers: Network services should only be obtained from service providers capable of providing relevant security controls, and be supported by documented contracts or service level agreements.
- 20.2 Third Party Access: Connections from third parties (i.e. external organizations, such as customers, suppliers and members of the public) should be subject to a risk assessment, approved by the application owner and agreed by both parties in a documented agreement, such as a contract.
- 20.3 Outsourcing: A process should be established to govern the selection and management of outsource contractors, supported by documented agreements that specify the security requirements to be met.

21 Business Continuity

- 21.1 Business Continuity: A business continuity plan should be developed, supported by contingency arrangements, and tested periodically.
- 21.2 Power Supplies: Critical computer equipment and facilities should be protected against power outages.