

EXHIBIT A  
P&G PRIVACY & SECURITY REQUIREMENTS

This document is in two parts: Privacy Requirements (“P&G’s Privacy Requirements”) and Security Requirements (“P&G’s Security Requirements,” together with P&G’s Privacy Requirements, the “P&G PRIVACY AND SECURITY REQUIREMENTS”).

P&G may modify these requirements from time to time to comply with PRIVACY LAWS. The modifications will be available on the Privacy Central website (<http://privacy.pg.com/privacy/index.shtml>). As a supplier you only need to enter the password pprivacy in the blank provided for vendors to access the website. It is the responsibility of the vendor to obtain access to the Privacy Central website to ensure they are operating under P&G’s current requirement: Contact your P&G business contact for access to the Privacy Central website.

**P&G’s PRIVACY REQUIREMENTS**

P&G’s Privacy Requirements 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.

P&G’s Privacy Requirements apply to SELLERS and SELLER’S REPRESENTATIVES who collect, use, transfer or store personal information. Before the SELLER and/or SELLER’S REPRESENTATIVES may collect, use, transfer or store P&G personal information they must have a valid contract, statement of work, or purchase order with the appropriate privacy and security language in place.

Simply put, P&G’s privacy goal is to protect, collect, and use personal information provided to us by others 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.

SELLER and SELLER’S REPRESENTATIVES agree to provide their services in accordance with the following provisions:

**1 Benefits for individuals:**

- 1.1 Minimum Necessary: Collection of personal information must 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 must 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 must be provided for all channels when collecting personal information. This notice must tell individuals what information P&G collects, 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 must 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 P&G does not have affirmative consent.
- 3.2 Clear and Obvious: Consent must 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 within other pages such as in Terms and Conditions. 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. 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.
- 3.3 Opt-out Provisions: Provide an "opt-out" option whenever contacting an individual for ongoing purposes. This opt out is required for all channels.
- 3.4 Processes for Opts: Verify that back-end processes are in place to process opts that are collected.
- 3.5 Suppression Lists: "Scrub" all outbound communication against appropriate suppression lists, including internal P&G lists and lists from external organizations, such as the DMA.
- 3.6 Current Best Approach: Consult Privacy Central for requirements, current approaches and appropriate wording for opts. 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 used 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 should 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 the new technology 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: Require two-factor authentication of SELLER and SELLER'S REPRESENTATIVE'S administrators, users and/or subcontractors when providing access to information online.

### 6 Security:

- 6.1 P&G Security Requirements: Follow the P&G Security Requirements section in this document for SELLERS and/or SELLER'S REPRESENTATIVES 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 or to satisfy relevant data retention laws.

### 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 P&G-approved industry standard encryption when collecting and transferring sensitive information.
- 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 (1) collect personal information online from individuals under the age of 13 or (2) provide P&G with personal information collected online from individuals under the age of 13.
- 8.2 Age/State Check: Verify that websites and other online programs do not collect personal information from individuals under the age of 13 by asking for birth date before collecting personal information. This includes mobile programs. Consult Privacy Central for appropriate wording for age checking and other requirements.
- 8.3 Approval to Collect: Obtain consent from the P&G country legal representative prior to collecting personal information from children not covered by section 8.1 above.
- 8.4 Minimal Collection: Where collecting personal information from children is allowed, ask only for the minimum information necessary for a child to participate in the program.
- 8.5 Parental Access: Where collecting personal information from children is allowed, implement a process that parents can obtain a copy of the information their child has provided, update the information, or ask us to no longer use the information.

## **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's Privacy Requirements 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 Privacy Requirements are implemented.
- 9.3 Privacy Training and Awareness: SELLER's employees and SELLER'S REPRESENTATIVES' employees must be made aware of the key elements of SELLER's privacy expectations and requirements and of their specific obligations with regard to providing compliant services pursuant to this AGREEMENT.
- 9.4 Privacy Compliance: Procedures must be in place to confirm that P&G programs are compliant with P&G's PRIVACY REQUIREMENTS 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 within 2 business days upon identification of incident.
- 9.6 Subcontractors: SELLER and/or SELLER's REPRESENTATIVES must have P&G's prior consent before providing any P&G personally identifiable information to a subcontractor. All subcontractors must also comply with Section 20.3 of P&G's Security Requirements.
- 9.7 Self-Assessment: Upon reasonable notice, SELLER's and/or SELLER's REPRESENTATIVES handling P&G personally identifiable information must complete P&G's vendor information privacy assessment to ensure they comply with P&G Privacy and Security Requirements.

## **SECURITY REQUIREMENTS (“P&G’s SECURITY REQUIREMENTS”)**

These Security Requirements apply to the service providers who collect, use, transfer or store PII or business information. Before SELLER can collect, use, transfer or store PII or P&G business information they must have a valid contract, statement of work, or purchase order with the privacy and security language in place.

P&G’s Security Requirements are based on the International Security Forum’s (ISF) Standard of Good Practice for Information Security and are consistent with the ISO/IEC 2700x series of standards for Information Security.

P&G’s Security Requirements are comprehensive in nature. Therefore P&G expects SELLER to also have a comprehensive set of policies, standards and controls to protect P&G’s information. SELLER must develop a data security program that documents the policies, standards and controls in use that relate to the provisions outlined below. This security plan must include organizational, administrative, technical, and physical safeguards and standards appropriate to the size and complexity, the scope of the activities and the sensitivity of the information at issue.

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

- (1) Ensure the confidentiality, availability and integrity of PII and P&G business information;
- (2) Protect against any anticipated threats or hazards to the confidentiality, availability or integrity of such information; and
- (3) Protect against unauthorized access to or use of such information.

*Also due to the inherent complexity associated with controlling information security risks, the SELLER and/or SELLER’S REPRESENTATIVE may be required to participate in an annual survey assessment for vendors known as the Full SIG described at <http://sharedassessments.org/products/sig-7-0-bundle/>.*

SELLER and SELLER’S REPRESENTATIVES agree to provide their services in accordance with the following provisions :

### **1 Information Security Governance**

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

### **2 Information Security Policy**

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

### **3 Security Education / Awareness**

- 3.1 Security Awareness: SELLER’S employees and SELLER’S REPRESENTATIVES’ employees must be made aware of the key elements of information security, why it is needed, and understand their personal information security responsibilities. Specific activities must 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 must be trained in how to run systems correctly and how to develop and apply security controls.

### **4 Accountability / Ownership**

- 4.1 Staff Agreements: Agreements must be established with SELLER’S employees and/or SELLER’S REPRESENTATIVES’ employees that specify information security responsibilities. This agreement must be

incorporated into the contracts of SELLER'S employees and/or SELLER'S REPRESENTATIVES' employees and be 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, must 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 must be subject to a formal risk analysis on a periodic basis, the results of which must be documented, reviewed, and agreed by the appropriate owner.
- 5.2 Confidentiality Requirements: When business information is stored in or processed by an application, the impact of business information being disclosed to unauthorized individuals must be assessed and discussed with P&G.
- 5.3 Integrity Requirements: When business information is stored in or processed by an application, the impact of business information being accidentally corrupted or deliberately manipulated must be assessed and discussed with &G.
- 5.4 Availability Requirements: When business information is stored in or processed by an application, the impact of business information being unavailable for any length of time must be assessed and discussed with P&G.

## 6 Asset Management

- 6.1 Security Classification: The application, computer installation and network must 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 must be used. This hardware/software must meet security requirements. Essential information about hardware, software, and data flows/extracts/interfaces (e.g., unique identifiers, version numbers, data recipients, physical locations) must be 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 (e.g., email, faxes, etc.) via secure file transfer protocols. Sensitive information is encrypted on all devices, including portable devices, such as laptops, portable media (flash drives) and data backups.
- 6.4 Acquisition: Robust, reliable hardware and software must 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 must be restricted to authorized individuals and enforced accordingly.
- 7.2 User Authorization: All users of the computer installation must be authorized before they are granted access privileges.
- 7.3 User Authentication: All users must 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 must 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 must 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 must be taken on a regular basis, according to a defined cycle discussed with and approved by P&G.
- 8.3 Web-enabled Applications: Specialized technical controls must be applied to web-enabled applications to ensure that the increased risks associated with web-enabled applications are minimized.
- 8.4 Ecommerce: A process must be established to ensure that information security is incorporated into electronic commerce initiatives enterprise-wide.
- 8.5 PCI Compliant: To the extent a SELLER and/or SELLER'S REPRESENTATIVE is acting as a Service Provider (as defined in the PCI Data Security Standards) on behalf of P&G and has access to cardholder payment card information including, but not limited to, account number, expiration date, or 3 or 4 digit CVV2 code, the SELLER and/or SELLER'S REPRESENTATIVE represents and warrants that it is a Level 1 PCI Compliant Service Provider, as defined at [http://usa.visa.com/merchants/risk\\_management/cisp\\_service\\_providers.html](http://usa.visa.com/merchants/risk_management/cisp_service_providers.html). To the extent a SELLER and/or SELLER'S REPRESENTATIVE is acting as a Merchant (as defined in the PCI Data Security Standards) on behalf of P&G and has access to cardholder payment card information including,

but not limited to, account number, expiration date, or 3 or 4 digit CVV2 code, the SELLER and/or SELLER's REPRESENTATIVE represents and warrants that it has assessed at the appropriate Level based upon its transaction volume, as defined at [http://usa.visa.com/merchants/risk\\_management/cisp\\_merchants.html](http://usa.visa.com/merchants/risk_management/cisp_merchants.html).

- 8.6 General Security Controls: The full range of general security controls must be considered when designing systems and services.
- 8.7 Application Controls: The full range of application and systems controls must be considered, and required controls identified and fully documented.

## 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) must be physically protected against accident or attack.
- 9.2 Hazard Protection: Computer equipment and facilities must be protected against fire, flood, environmental and other natural hazards.
- 9.3 Power Supplies: Critical computer equipment and facilities must be protected against power outages

## 10 System Configuration

- 10.1 Host System Configuration: Host systems must 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 must be purchased from a list of approved suppliers, tested prior to use, supported by maintenance arrangements, and protected by controls such as malware, anti-virus, software firewall, and host intrusion protection software.
- 10.3 Configuration of Network Devices: Network devices must 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 must 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: Event Logging: Logs of all key events, including but not limited to (i) user times/dates of access, session duration and activities (files created, deleted, edited, reviewed); (ii) application administrator activity including times/dates of access, session duration and activities (configuration changes and user administration); and (iii) system administrator access and activities on the server 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 must be monitored continuously, and from a business user's perspective.
- 11.3 Intrusion Detection: Intrusion detection mechanisms must be applied to critical systems and networks.

## 12 Network Security

- 12.1 Installation and Network Design: Systems must be designed with sufficient capacity to cope with predicted information processing requirements. Systems must be protected by using a range of in-built security controls.
- 12.2 Network Documentation: Networks must be supported by accurate, up-to-date documentation.
- 12.3 External Access / Connections: All external connections to the network must be individually identified, verified, recorded, and approved by the network owner.
- 12.4 Firewalls: Network traffic must be routed through a firewall, prior to being allowed access to the network.
- 12.5 Wireless Access: Wireless access must 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) must be monitored regularly and access to them restricted.
- 13.2 Email: E-mail systems must be protected by a combination of policy, awareness, procedural and technical security controls.
- 13.3 Instant Messaging: Instant Messaging systems must be protected by a combination of policy, awareness, procedural and technical security controls.

## 14 Cryptography

- 14.1 Cryptography: Cryptographic solutions must be approved, documented and applied enterprise-wide.
- 14.2 Public Key Infrastructure: Where a public key infrastructure (PKI) is used, it must 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 must be established and security controls for handling personally identifiable information applied and documented.
- 15.2 Alignment with P&G Privacy: Personally identifiable information is collected, used, stored, transferred, and destroyed according to P&G's Privacy Requirements.

## 16 Malware Protection

- 16.1 Virus Protection: Virus protection arrangements must be established, and maintained enterprise-wide.
- 16.2 Malicious Code Protection: Enterprise-wide arrangements must 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 must be carried out in accordance with a documented system development methodology. System development activities must 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 must be performed during the development lifecycle.
- 17.3 Specification of Requirements: Business requirements (including those for information security) must be documented and agreed before detailed design commences.
- 17.4 System Design / Build: Information security requirements for the system under development must be considered when designing the system. System build activities (including coding and package customization) must 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) must be tested before the system is promoted to the live environment.
- 17.6 System Promotion Criteria: Rigorous criteria must be met before new systems are promoted into the live environment.
- 17.7 Installation Process: New systems must be installed in the live environment in accordance with a documented installation process.
- 17.8 Post-implementation Review: Post-implementation reviews must 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 must be tested, reviewed and applied in accordance with documented standards/procedures
- 18.2 Change Management: Changes to any part of the computer installation must be tested, reviewed and applied using a change management process.
- 18.3 Patch Management: There must be a strategy for patch management and a documented patch management process.
- 18.4 Remote Maintenance: Remote maintenance of the network must 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 – must be recorded, reviewed and resolved using an incident management process.
- 19.2 Alignment with P&G Privacy: Incidents must be reported to P&G immediately.
- 19.3 Forensic Investigations: A process must be established for dealing with incidents that require forensic investigation.

## 20 Third Party Management

- 20.1 Service Providers: Network services must 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) must be subject to a risk assessment, approved by the application owner and agreed by both SELLER and P&G in a documented agreement, such as a contract.

- 20.3 Outsourcing: A process must be established to govern the selection and management of outsourced contractors. These outsourced contractors must sign agreements that specify the security requirements to be met before commencing work on behalf of P&G.

## **21 Business Continuity**

- 21.1 Business Continuity: Business continuity and IT Disaster Recovery plans must be developed, supported by contingency arrangements, and tested periodically.

## **22 Processing Facility for servers, including cloud security requirements**

- 22.1 Any P&G data stored on a cloud environment must be encrypted either by the vendor or the application so that data cannot be read by other users in a multi-tenant environment.
- 22.2 When PII or P&G business information is co-located with non-P&G data, (e.g., virtual servers, cloud solutions, etc.) the non-P&G data must be logically separated from the PII and/or P&G business information.
- 22.3 Sensitive business information copied from the production environment must be protected by depersonalizing sensitive business information, restricting access to business information in the development environment, or erasing copies of business information once testing is complete.
- 22.4 Before relocating the physical storage location of PII and/or P&G business information to a country different from the ones documented in the statement of work or contract, the P&G party must be notified in advance so that potential implications for privacy can be addressed.

## **23 Authentication**

- 23.1 Websites and shared document areas containing PII and or P&G business information must implement user-authentication (i.e., individual user IDs and passwords), not group or shared account authentication. Consumers may provide their own data in accordance with the privacy requirements for the individual site.
- 23.2 Strong authentication is required for privileged access to servers and applications hosting P&G data.