P&G Privacy Policy

PFC Privacy Policy

PEP Privacy Policy

TPG Privacy Policy

P&G Global Consumer Privacy Policy

5/25/2018

We work hard to build and maintain a relationship of trust with you. So, when it comes to handling your information, we do so carefully and sensibly, and in ways that live up to that trust. This policy lets you know how we do that, including what information we collect, how we use and protect it, and how you can decide what we do with it. Our goal is to help you understand how we use your information to improve our content, products, advertisements, and services.

Here's a short introduction to our privacy practices

what we collect:

- Information you give us
- Information we collect when you contact us, visit our sites, use our mobile applications or services, use our products or devices, or view our advertisements
- Information we get from other companies who have obtained your consent to share or sell it or have ensured that other companies from whom they have received your information can share it with them and, in turn, with us and/or other companies
- Information we get from other companies when you visit their websites

We may combine any and all of this information to help create better products, services, and consumer experiences.

how we use your information

- Send you the products and services you ask for
- Tell you about our and our marketing partners' products and services
- Help us run our sites and services

how and when we share your information

- When we have your consent, with our carefully selected partners so that they can send you offers, promotions, or ads about their products and services we believe you may be interested in
- With other companies we hire to help us run our business
- As part of a sale of a P&G brand or business to another company
- To help us protect our rights or property, e.g., fraud prevention or information security
- When required by law or government authorities

your choices

- You can tell us how we can use your information by clicking on the links below:
- Marketing communications
- Interest-based advertising

If you live in the EU, you have certain personal data rights, including to access what personal information we have about you, make corrections or updates to it, tell us to delete that data, or receive a portable copy of that information. These rights don't apply in all situations. Please click the links below to:

- Access or update personal information
- Request correction, deletion, or transfer of your personal information

How We Collect Your Information

We collect information about you in many ways from many places. Some of the information we collect may include personal information that can be used to identify you; for example, your name, email address, telephone number, or postal address. In some countries like those in the EU, things like IP address or cookie and mobile device identifiers may also be considered personal information.

Please note: We may combine all of the information we collect about you to give you better products, services, and user experiences.

you provide it to us. You give us your information when signing up for an account on our websites or in mobile apps or by calling or emailing us. We may ask for things like your name, email or home address, date of birth, payment information, your age, gender, the number of people in your family, and the way you want us to send you information about our products and services—for example, to your home address, email address, or by texting you.

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

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

from other places. We may get information that other companies share with or sell to us. For example, you may have given consent for another company to share your personal information with us when you signed up for telecom services or a retailer loyalty points program. We may also collect information from places that you know everyone can see, such as from internet postings, blog entries, videos, or social media sites. We may also receive information from other companies who are in the business of collecting or aggregating information about you sourced from publicly available databases or from consent you have given to their use and subsequently our use of your information. This might be information about your income level, age, gender, number of people in your family, and products you have bought on the internet or from stores in your neighborhood.

How We Use Your Information

We use your information to help us meet our purpose of touching and improving the lives of people like you every day around the world. We use your information to respond to your questions or requests for information, send you products or samples you have requested, help you manage your P&G site or app preferences, allow you to enter our contests or sweepstakes, or process your payment for the products you buy from us. We may also use your non-personal information (e.g., purchase data, sample requests, etc.) in consumer research or analytics (or personal information when you have consented to participate in such research) to learn more about what consumers want so that we can make new products or improve the ones we already have.

Another way we use your information is to make sure that what you hear from us is relevant and useful to you as an individual. For example, we may send you information about Gillette® products if you have shown interest in our shaving products by visiting Gillette.com. When we do this, we will use your information – a cookie ID or device ID -- to limit the number of times you see the same advertisement from Gillette. We want you to hear from us about the products you use and love without you hearing the same message over and over again.

We may also use aggregate information from many people without identifying any individuals to better understand how our websites are being used or to study consumer habits so that we can make products and offer services that meet the needs of all consumers sharing some of the same things in common. For example, we can learn a lot about consumers who are new parents reading our baby product websites, so that we can better serve new parents everywhere with the products and services they want. Use of such non-personal information in this way helps to safeguard your privacy. We will always try to use non-personal information whenever possible for this reason.

To further protect your privacy, we will also use the least amount of information we can to accomplish the task at hand, put measures in place to prevent mixing information in ways that would allow cookie and device IDs to specifically and directly identify you (e.g., by name), and delete your information when we no longer need it for our business purposes.

How We Safeguard Your Information

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

What We Share

with other companies. When we have your consent, we may share your information with select partners so they can send you offers, promotions, or ads about products or services we believe you may be interested in. For example, people who receive P&G emails from our diaper brands such as Pampers® may also consent to hear about baby formulas made by other companies. We do not sell your personal information to marketers outside of P&G. We may share information that does not personally identify you with other companies for any purpose.

with service providers. We may need to share your information with companies who help us run our business, including hosting our sites, delivering our emails to you, analyzing the data we collect, and sending you the products and services you requested. We share only the personal information needed for these companies to complete the tasks we request. They are required to protect your information in the same way we do and will not share it or use it for any other purpose.

other situations. If a brand or one of our businesses with which you've shared personal data is sold to another company, your data will be shared with that company. As a result, your account and the personal data in it will not be deleted unless you tell the brand or new company that you want it deleted. We may also share your information with companies who help us protect our rights and property, or when required by law or government authorities.

Your Rights and Choices

marketing You can tell us to stop sending you email and text messages by following the opt-out instructions sent with these communications. You can also choose to stop receiving marketing email, SMS, or postal mailings by clicking here. While we will honor your choices, we may need to keep information to do so. For example, if you tell us to stop sending marketing emails, we will need your email address on file so that our systems remember that you no longer wish to receive marketing communications to that email address.

accounts Depending upon the country where you registered, your P&G account may offer the ability to access your information and make updates to or delete your data. If not, you can click here to make a request.

european union residents. If you live in the EU, you may access the personal data we hold about you, request that inaccurate, outdated, or no longer necessary information be corrected, erased, or restricted, and ask us to provide your data in a format that allows you to transfer it to another service provider. You also may withdraw your consent at any time where we are relying on your consent for the processing of your personal data. And you may object to our processing of your personal data (this means ask us to stop using it) where that processing is based on our legitimate interest (this means we have a reason for using the data). If you would like more information about data protection and your personal data rights in general, please visit the European Data Protection Supervisor's site at https://edps.europa.eu/data-protection/.

If you are not happy with our response to your requests, you may lodge a complaint with the data protection authority in your country. Please select from the following options to make your request:

general requests . To make a request with respect to personal data used for marketing, which would include for example information you provided us as you registered through one of our websites or apps, please contact us here.

media advertising . To make a request with respect to personal data used for advertising, which would include for example information we may have about you at a cookie or device ID level and which we use to provide you with relevant ads, please contact us here . There may also be data associated with your cookie or device ID in our demand-side (or ad-serving) and ad verification partner platforms. For that data, please see here and here.

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

dental professionals. If you are a dental professional and have provided your information to us as part of one of our professional outreach programs, including through https://www.dentalcare.com, please contact us through the appropriate country numbers and email addresses listed below.

Country	Call Center	E-mail
Germany	0203 570 570	N/A
Austria	00800 570 570 00	N/A
Switzerland	00800 570 570 00	N/A
UK	0870 242 1850	Click here
Spain	900 670 270	Click here
Italy	+390650972534	N/A
France	+ 33 (0) 825 878 498	Click here
Belgium	N/A	Click here
Netherlands	N/A	Click here
Poland	0 801 25 88 25	N/A
Sweden, Norway, Denmark, Finland	N/A	Click here

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 and letters (e.g., cookie ID ABC12345) and never as, for example, John E. Smith.

We use cookies for a number of reasons, such as:

- to serve you with relevant advertising
- to learn more about the way you interact with P&G content
- 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

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. For example, session cookies are extremely helpful when shopping online—without them the items you place in your shopping cart would disappear by the time you reach the checkout! 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.
- **advertising cookies.** These cookies can be used to learn about what interests you generally might have, based, for example, on the websites you visit and the products you buy. This can also help us infer things about you such your age, marital status, and how many kids you may have. That data allows us to send you ads for products and services that better fit the things you like or need. It also allows us to limit the number of times you see the same advertisement.
- **analytics cookies.** These cookies tell us how our websites are working. In many cases, we use Google analytics cookies to monitor the performance of our sites. Our ability to use and share information collected by Google Analytics about your visits to our sites is restricted by the Google Analytics Terms of Use and the Google Privacy Policy .

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

Other Technologies.

- **proximity-based beacons.** Beacons send one-way signals to mobile apps you install on your phone over very short distances to tell you, for example, what products are on-sale as you walk through a store. Beacons only talk to your device when you get close enough and after you have given consent within the mobile application associated with a particular beacon. In turn, apps may provide us location information to help customize advertising and offers to you. For example, when you are near a beacon in the skin care section of a supermarket, we may send you a $4 off coupon.
- **pixels.** These are small objects embedded into a web page, but are not visible. They are also known as "tags," "web bugs," or "pixel gifs." We use pixels to deliver cookies to your computer, monitor our website activity, make logging into our sites easier, and for online marketing activity. We also include pixels in our promotional email messages or newsletters to determine whether you open and act on them.
- **mobile device identifiers and SDKs.** We use software code in our mobile apps to collect information similar to what cookies collect on the internet. This will be information like your mobile phone identifiers (iOS IDFAs and Android Advertising IDs) and the way you use our apps. Similar to cookies, the device information we collect automatically as you use our apps will never identify you as a person. We only know a mobile device as randomly assigned numbers and letters (e.g., advertising ID EFG4567) and never as, for example, John E. Smith.
- **precise geolocation.** We may receive information about your exact location from things like global positioning system (GPS) coordinates (longitude and latitude) when you use our mobile apps. You will always get a pop-up notice on your phone or device asking for you to accept or reject allowing us to know exactly where you are in the world. You should understand that we will not always ask for consent to know generally that you are in a broader city, postal code, or province. For example, we do not consider it to be precise location if all we know is that you are somewhere in Manila, Philippines.

Interest-Based Advertising

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

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

we link other information to your cookie and device IDs. Your cookie and device IDs may be supplemented with other information, such as information about the products you buy offline or information that you provide directly to us when creating an account on our sites. We generally do this in ways that will not directly personally identify you. For example, we could know that cookie ID ABC12345 belongs to the razor aficionado group based on person's web site visits, age, gender, and shopping habits, but we would not know that person's name or address or other information that would identify him or her as a person. Should we ever want to personally identify your cookie or device information (web and app viewing history), we will always ask you before doing so.

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

how you can stop receiving interest-based ads. To stop receiving P&G interest-based advertising, you can click here or click on the WebChoices or AppChoices icons on one of our sites or in one of our mobile applications. You can also prevent getting interest-based ads on websites by declining cookies in your browser(s), declining the "access to data" requests that apps usually present when you install them, or by adjusting the ad tracking settings on your device.

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

deleting cookies also deletes your opt out. When you opt out of interest-based advertising, we send an opt-out cookie to your browser that tells us that you no longer want to receive interest-based ads from us. Your opt-out cookie will be deleted if you decide to delete all cookies. This means that you will need to opt-out again if you still do not want to receive interest-based ads.

European Union Data Processing, Retention, and Transfers

This section applies only to our processing of personal data of EU country residents. It aims to provide increased transparency into our processing, retention, and transfer of EU resident personal data that is in line with the letter and spirit of the General Data Protection Regulation.

entities. Different P&G entities may be the controller of your personal data. A data controller is the entity which directs the processing activity and is principally responsible for the data. The chart below identifies our data controllers for EU country data. For example, when you register for email on one of our French (.fr) websites, the P&G entity listed next to that country name will be the controller of that personal data (e.g., Procter & Gamble France SAS (LE 577).

Countries	Data Controller
Austria	Procter & Gamble Austria – Zweigniederlassung der Procter & Gamble GmbH
Bulgaria	Procter & Gamble Bulgaria EOOD
Romania	For contests: Procter & Gamble Distribution SRL For other sites: Procter & Gamble Marketing Romania SR
Poland	Procter and Gamble DS Polska sp z o.o.
Belgium	Procter & Gamble Distribution Company (Europe) BVBA For P&G Healthcare: P&G Health Belgium BVBA, Temselaan 100, 1853 Strombeek-Bever
Czech Republic	Procter & Gamble Czech Republic s.r.o.
Hungary	Procter & Gamble RSC Regionális
Slovakia	Procter & Gamble, spol. s.r.o.
Croatia	Procter & Gamble d.o.o. za trgovinu

France	Procter & Gamble France SAS/Procter & Gamble Pharmaceuticals France SAS" For P&G HealthCare as of 1 July '19 : P&G Health France S.A.S., 163 Quai Aulagnier, 92600 Asnières-sur-Seine
Germany	Procter & Gamble Service GmbH For P&G HealthCare: P&G Consumer Health Germany GmbH, Sulzbacher Strasse 40, 65824 Schwalbach am Taunus
Greece	P&G Hellas Ltd.
Ireland	Procter & Gamble UK
Italy	Procter & Gamble Srl
Netherlands	Procter & Gamble Nederland B.V.
Portugal	Procter & Gamble Portugal, Productos de Consumo Higiene de Saude, S.A.
Spain	Procter & Gamble España, S.A.
United Kingdom	Procter & Gamble UK Seven Seas Limited, The Heights, Brooklands, Weybridge, Surrey KT13 0XP
EU Countries Not Listed	Procter & Gamble International Operations SA

processing and retention. As a general rule, we keep your data for only as long as it is needed to complete the purpose for which it was collected or as required by law. We may need to keep your data for longer than our specified retention periods to honor your requests, including to continue keeping you opted out of marketing emails, or to comply with legal or other obligations. This chart tells you the type of data we collect, the purposes for which we use it, why such uses comply with the law (legal basis), and how long we usually keep it (retention period).

Type of Data	Why We Collect This Data	Legal Basis	Retention Period
Marketing Email, name, phone number, postal address, your affinities, your interests, your profession, your habits, what you bought, the photos or videos you upload, information about your children and your home, your family composition, the number of people in your household, your hair type, your skin type, your favorite scent, whether you have a pet, etc.	To send you materials marketing our products or services or the products or services of our partners.	Your consent for email and SMS and, where we obtain it, consent for postal. Legitimate interests for everything else.	Until you request to delete the personal data or withdraw your consent. If you do not make such a request, the personal data will be deleted on the following schedule: email: after <50 months of all- channel inactivity. We define inactivity through several internal criteria. SMS: after <50 months of all- channel inactivity. We define inactivity through several internal criteria. postal address: after <50 months of all-channel inactivity. We define inactivity through several internal criteria.
Contests Email, name, phone number, sometimes other data.	To provide contest participants with information about the contest, including announcing the winner(s) of the contest.	Your consent.	For 24 months unless local law requires us to retain it longer.
Product Purchases Email, name, phone number, payment information (including bank account IBAN or Paypal details), sometimes other data.	To process your purchases of our products, cashback offers, or warranties and to send you relevant communications related to that purchase.	Your consent.	As long as necessary to fulfill your order and follow up with communications about your order unless local law requires us to retain it longer. We also generally retain data for 24 months for cashback offers and 10 years for warranties.
Contact Us Email, name, phone number, sometimes other data.	To address your inquiries and make sure we follow up appropriately or as may be required by law or P&G policy.	Our legitimate business interest in managing consumer inquiries, as well as your consent for special category data which may be collected in some adverse event cases.	From 0 to 10 years, depending on the nature of the inquiry, our legitimate interests for processing the data, and our legal obligations.
Research Email, name, phone number, address, identifiable photos or videos, sometimes other data.	To test our product ideas and learn about your preferences and practices so that we can improve our products and the lives of our consumers.	Your consent.	We will retain the personal data collected as part of substantive clinical research for as long as we need it for the purpose for which it was collected, and/or for as long as may be required to retain it by local law or regulation, which may be up to 25 years. For non-clinical research, we will retain your substantive personal data for a maximum of 5 years. We will retain your signed informed consent documents
Media Targeting Advertising cookies, device ID, demographic information such as gender and age, behavioral data	To learn about your Internet interests and customize the ads we send you.	Our legitimate business interests in serving you with relevant advertising. We	We will retain this data for thirteen months from the date we collect it or until you opt out, whichever is earlier.
such as page views, and sometimes other data.		will obtain your consent for the deployment of cookies on our own websites.	

transfers of your data to other countries. Your personal information may be transferred to, stored, and processed in a country other than the one in which it was collected, including the United States. For example, we may store your data on a server in the United States because that is where a particular database is hosted; and that data may be "transferred" again when one of our marketers accesses that data from Switzerland to send you a product sample. We perform such transfers, both between 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 model contract clauses). If you would like a copy of a transfer agreement, contact us.

Site and App Content

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

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

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

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

Children's Privacy

children's online privacy laws. We follow all applicable data protection laws when collecting personal information online from children. For example, in the EU we do not collect personal information from children under 16 years of age unless we get consent from a parent. Similarly, in the U.S., we obtain verified parental consent when collecting personal information from children younger than 13.

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

Contact Us

Please contact us directly with any questions or concerns you may have about your privacy and our data protection practices.

PROMOTION FULFILLMENT CENTER PRIVACY POLICY

PRIVACY POLICY

How PFC gathers and disseminates information collected through our websites is described below. Use of PFC websites is subject to the “Terms and Conditions of Use” below as well. This Privacy Policy only governs our use of the information we collect online and does not govern the use of information we may collect in other ways.

HOW WE COLLECT INFORMATION

We collect information you post or submit through the PFC websites. For example, we collect information from you when you submit our “contact us” form. We also collect information you submit to claim a rebate, to enter a sweeps, or to order a product, or if you contact customer service. We may collect information from you passively: we use tracking tools and web beacons. The information we collect passively explains the frequency of visits to certain web pages, the effectiveness of our search terms and any other procedures we are using to drive traffic to our web site. We may collect demographic information to combine with other information for statistical and analytical purposes. This website is not directed at persons under the age of thirteen (13), and PFC does not solicit or knowingly collect personally identifiable information on anyone under the age of 13. If you are a parent and you think your child under 13 has given us personally identifiable information, you can email us here: info@pfcfulfills.com. Please mark your inquiry as “COPPA Information Request.” PFC has no way to verify the age of persons accessing our websites. We may also collect information about you through third parties: our clients, vendors and others.

HOW WE USE INFORMATION

We use your information for transactional communications: to process your orders, rewards, prizes and promotions and for legal compliance. We use it to respond to your requests or questions. We may also use it for security purposes. We may also use portions of your information, such as name, address, email and phone, to study the effectiveness of our campaigns, improve our websites, and determine customer satisfaction. We may send you information about our future programs. You may always opt out of receiving future communications. *See Opt Out Choices below*.

We may use information that is not considered personally identifiable information for any purpose. We may use it to improve our products and services, and to make our website better. We may combine information we get about you with information about you from third parties.

We may share information with third parties who perform services on our behalf. If we collect your information on behalf of a client, we may share your information with the client. We may also share your information to comply with the law or to protect ourselves. We may share information with any successor to all or any part of our business. For example, if part of our business was sold, we may include data we have collected from you as part of that transaction. We may share information for other reasons we may describe to you. We will not sell your information to unaffiliated third parties.

If you reside in California, you have the right to ask us one time each year if we have shared personal information with third parties for their direct marketing purposes. To make such a request, send us an *email at info@pfcfulfills.com*, or write us at this address: "Shine the Light" inquiry, c/o PFC, 311 21st Street, Camanche, IA 52730 ATT: Legal.

LINKS AND THIRD PARTY PRIVACY POLICIES

Our websites may contain links to other sites or services not operated by PFC and over which PFC has no control. We are not responsible for the privacy practices or contents of such other websites. You should review the respective privacy policies of any links you follow.

Our site may also serve content or third party ads that contain their own cookies or tracking technology. We do not control the use of such technologies. Such ads may be based on information collected by us, by third parties or information collected by your activities on our websites or on the websites of others.

SECURITY MEASURES

Our website has reasonable security measures in place to help protect against the loss of information under our control.

Use of the internet is never 100% secure. Though we strive to protect your information, we cannot warrant the security of any information you transmit to us. Should you determine that your data has been compromised, please notify PFC immediately by phone at: 563-259-0105, ATT: Legal, or email:info@pfcfulfills.com with the header: Data Compromised.

INFORMATION STORED BOTH INSIDE AND OUTSIDE US

We store information both inside and outside the U.S. PFC websites are subject to U.S. laws, which may not afford the same level of protection as the laws of other countries.

OPT OUT CHOICES

When you submit information about yourself on our website, we may send you emails or otherwise contact you on behalf of our clients with respect to promotions and products of interest or products you have ordered. You may opt out of receiving commercial email communications from PFC and this option will be included as a link on any email communication we send you. If you opt out, PFC will not send you any further marketing communications on our behalf or on behalf of our clients. We may still need to contact you to fulfill the administrative components of any program or promotion in which you are participating or to fulfill your order. Any opt out request will be fulfilled as soon as reasonably possible.

UPDATES TO THIS PRIVACY POLICY

From time to time we may change our privacy policy. You may check the “Last Updated” information at the bottom of this site. Any updated policy will be posted on our websites.

CONTACT US

If you have any questions about this policy or other privacy concerns, email us at:info@pfcfulfills.com. You may also write us at: PFC, Privacy Policy, 311 21st Street, Camanche, IA 52730, ATT: Legal.

TERMS AND CONDITIONS OF USE

Your right to use PFC websites is limited to personal and non-commercial use:

- YOU MAY NOT USE OUR WEBSITES FOR COMMERCIAL USE.
- YOU MAY NOT MODIFY ANY CONTENT YOU DOWNLOAD OR PRINT FROM OUR SITES.
- YOU MAY NOT INTERRUPT OR ATTEMPT TO INTERRUPT THE OPERATION OF ANY OF OUR WEBSITES IN ANY WAY.
- YOU MAY NOT USE OUR WEBSITES FOR ANY ILLEGAL PURPOSES.
- YOU MAY NOT STORE THE CONTENT OF OUR WEBSITES IN A DATABASE.
- YOU MAY NOT MODIFY THE CONTENTS OF OUR WEBSITES.
- YOU WILL NOT ALLOW OTHERS TO USE YOUR USER NAME AND PASSWORD.

The content on our websites is provided “as is,” and without warranties of any kind, express or implied. PFC does not in any way warrant or represent that the content of our websites will be complete or accurate. PFC does not represent or warrant that our websites will work with your computer, will work without error, or will be free from destructive viruses or other harmful components. PFC will not be liable to any party for any damage of any kind for use or reliance upon the content of our websites.

TO THE FULLEST EXTENT PERMITTED BY LAW, PFC DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING IMPLIED WARRANTIES OF

FITNESS FOR A PARTICULAR PURPOSE AND IMPLIED WARRANTIES OF MERCHANTABILITY. PFC will not be liable for any damages of any kind arising from the use of our sites, the content thereof, or the services offered thereby, including, without limitation, indirect, direct, punitive, consequential or other types of damages. RISK OF USE OF OUR WEBSITES IS WITH THE USERS.

PFC disclaims any responsibility for the accuracy, content, security, or use of information found on links to third parties from our websites over which we have no control.

YOUR USE OF OUR WEBSITES

Your use of our websites denotes your acceptance of our Privacy Policy and Terms and Conditions of Use.

Last Updated: November 21, 2016

PEP Privacy Policy
4/10/2019

EXHIBIT A

PEP DATA PRIVACY & INFORMATION SECURITY REQUIREMENTS

PEP Data Privacy & Information Security Requirements ("Privacy Requirements") are intended to be consistent with industry standard data privacy standards and apply to each provider of goods or services to PEP ("SELLER") and any of SELLER'S representatives ("SELLER'S REPRESENTATIVES") who collect, use, transfer or store Personally Identifiable Information in connection with the services SELLER provides under the Agreement and are intended to reflect the privacy requirements of its customers (each, a "BRAND"). It is the policy of PEP not to do business with any SELLER that would require the collection, use, transfer or storage of any Personally Identifiable Information unless the SELLER has agreed to these Privacy Requirements.

PEP may modify the Privacy Requirements from time to time. The modifications will be available on www.pepconnect.com/pdf/privacy.pdf (the "Site"). As a supplier you only need to enter the password "peppromotions" in the blank provided for vendors to access the website. It is the responsibility of each SELLER to regularly access the Site and review the Privacy Requirements from time to time to ensure they are operating under PEP's current requirements. The following Privacy Requirements may be referenced in and, regardless, are a supplement to the terms of the SELLER'S agreement with PEP for goods or services – i.e., either the PEP "Terms and Conditions for Purchase of Goods/Services (accessible at https://www.pepconnect.com/TermsAndConditions - password is "peppromotions") or the current Master Operating Agreement between SELLER and PEP ("Agreement"). Contact your PEP business contact if you have any issues accessing the Site or the Agreement. In the event of a conflict between the terms in the Agreement (including any specific privacy provisions in the Agreement) and these Privacy and Information Security Requirements, the terms of these Privacy and Information Security Requirements will govern.

PEP DATA PRIVACY REQUIREMENTS

PEP's privacy goal is to protect, collect, and use Personally Identifiable Information consistent with the privacy policy of the BRAND to which PEP and SELLER are providing goods and services ("Brand Privacy Notice"). "Personally Identifiable Information" or "PII" is either (i) as defined in the applicable Brand Privacy Policy; or, if no Brand Privacy Notice applies, (ii) any information that (a) independently identifies a distinct individual, or (b) in combination with information readily available to us can be used to identify a distinct individual, or (c) would be considered personal information or personal data as those terms or similar terms are defined by applicable law. It includes but is not limited to, name, mail address, email address, social security number, financial account or card information, phone number, password, and entity affiliation. "Highly restricted information" or "HRI" means any BRAND Information identified as being highly restricted (or confidential) either by label on the information/media or by type as identified in a writing. "Brand Information" means any BRAND data or information, including Personally

Identifiable Information or HRI used, created or accessed in the performance of services for or on behalf of a BRAND.

The Privacy Requirements described below are comprehensive in nature, and each SELLER should develop a privacy program that incorporates the following fair information practice principles (FIPPs) as appropriate to the size and complexity, the nature and scope of the activities, and the sensitivity of any Personally Identifiable Information that it processes:

- Notice and Awareness
- Choice and Consent
- Access and Participation
- Integrity and Security

In keeping with these FIPPs, PEP adheres to the following practices, and expects SELLERs to adhere to them as well:

- We use Personally Identifiable Information, HRI and Brand Information only for purposes consistent with the reason it was provided.
- We do not share Personally Identifiable Information, HRI or Brand Information with other marketers.
- Our Privacy Requirements apply to:
    - All Personally Identifiable Information collected from individuals (whether from consumers, customers, and research subjects) who do business with a BRAND.
    - All locations where we operate.
    - All methods of collection such as 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. Processing: SELLER will process Personally Identifiable Information solely for the purposes described in the Statement of Work attached to the Agreement.
    1.2. Minimum Necessary: Collection of Personally Identifiable Information must be limited to the minimum amount of such information necessary to meet the needs of the BRAND program; do not collect any information that is not needed.
    1.3. Plan for Use: Collection of Personally Identifiable Information must be limited to what is necessary to provide the agreed to services. Do not collect Personally Identifiable Information if there is no plan in place to use that information. This is necessary to reduce the chance of misuse or unauthorized use of the Personally Identifiable Information.
    1.4. Collected Purpose Only: Use of Personally Identifiable Information is limited to the purpose for which it was collected as reflected in the privacy notice described in Section 2. Such

information may only be used for the purpose for which it was collected in accordance with PEP or BRAND instruction and never in a manner that violates applicable law or is not consistent with these Privacy Requirements.

1.5. Not Shared: Personally Identifiable Information that is collected under a BRAND program is owned by the BRAND, and SELLER acknowledges that it has no rights to or ownership interest in any such information. Personally Identifiable Information may not be distributed, sold, licensed, leased, or shared with any other persons, such as other marketers, agents or contractors without the prior written consent of PEP.

2. Notice:

2.1. Notice at Collection: The Brand Privacy Notice must be provided by SELLER for all delivery channels when collecting Personally Identifiable Information in connection with a BRAND program. This notice must tell individuals what information the BRAND 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 the BRAND with privacy questions.

2.2. Notice at Use: The Brand Privacy Notice must be provided whenever an individual is contacted.

2.3. Acceptable Notice: The Brand Privacy Notices is typically set forth on the BRAND's website. SELLER shall contact PEP for any necessary direction on the appropriate privacy notice. In the event no Brand Privacy Notice applies, you must post the privacy notice supplied to you by PEP. You must obtain PEP's written permission for proposed variances from current processes and procedures listed on the Site.

3. Choice:

3.1. Affirmative Consent: You must obtain affirmative opt-in to use the Personally Identifiable Information collected in connection with the BRAND program for specified purposes, and to contact the individual in the future. Do not contact individuals where the BRAND does not have affirmative consent to be contacted by the BRAND via the applicable channel.

3.2. Clear and Obvious: Consent must be requested in a clear and conspicuous manner using easily understandable language, and the request for consent must be provided at the time and place the Personally Identifiable Information is collected, 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.

3.3. Consent Based Contact: Contact only individuals who have agreed to be contacted. For example, use purchased lists of names only from providers who represent that they have verified that the listed names have consented to hearing from companies such as the relevant BRAND.

3.4. Co-marketing Arrangements: Obtain PEP's written guidance for all co-marketing efforts (where consumers may be opting in to both a BRAND'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 immediately process opts that are collected.
3.7. Suppression Lists: "Scrub" all outbound communication against appropriate suppression lists, including internal PEP and BRAND lists and lists from external organizations, such as the Digital Marketing Association (DMA).

4. Technology:
4.1. Privacy-Impacting Technologies: Notify individuals of all technologies that you are using to collect Personally Identifiable Information (e.g., Caller ID, etc.). Do not use technologies that the individual may not be aware of to collect Personally Identifiable Information.
4.2. No Information on Individual's Computer: Cookies, files or other technologies stored on an individual computer in connection with BRAND programs should never collect or contain Personally Identifiable Information.
4.3. New Technologies: Obtain permission from PEP when utilizing any new technology to collect Personally Identifiable Information, store Personally Identifiable Information, or track Personally Identifiable Information to verify the new technology is consistent with PEP's Privacy Policy and, as applicable, any Brand Privacy Notice.

5. Data Accuracy & Access:
5.1. Correct Information: Take appropriate steps to make sure that the Personally Identifiable Information used is correct.
5.2. Correct Lists: Use good lists; make sure that purchased lists use valid data, both the Personally Identifiable 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 Personally Identifiable Information.
5.5. Update to Information: Where applicable, ensure a process is in place for individuals to update and correct their Personally Identifiable Information as may be needed.
5.6. Online Access: Require two-factor authentication of SELLER and SELLER'S REPRESENTATIVE'S administrators, users and/or authorized subcontractors when providing access to any type of information online.
5.7. Subject Access Rights. SELLER shall assist PEP and BRAND as reasonably requested by implementing appropriate technical and organizational measures for the fulfillment of the BRAND's obligations to respond to requests from data subjects to exercise their rights, where relevant and required by applicable law, in respect of their Personally Identifiable Information, including but not limited to the right to access the PII processed by SELLER and to request the

rectification of inaccurate PII. SELLER shall not directly respond to any such request from a data subject without the express prior written consent of PEP and BRAND.

6. Security:
   6.1. PEP Security Requirements: SELLERS and/or SELLER'S REPRESENTATIVES must follow the PEP Security Requirements section in this document to protect Personally Identifiable Information, HRI and Brand Information by use of industry standard information security practices and measures, in order to prevent loss, misuse, unauthorized access, disclosure, or alteration. In particular, SELLER will utilize organizational, administrative, technical and physical safeguards to protect Brand Information consistent with current accepted industry standards (e.g., the NIST Cyber Security Framework (ISO27001/27002).
   6.2. Control Access: Limit and/or restrict access (including administrative access) to Personally Identifiable Information to those who have a business need.
   6.3. Data Retention: Delete data when it is no longer needed; do not keep Personally Identifiable Information any longer than necessary to meet the business need or to satisfy relevant data retention laws, and under no circumstances retain Personally Identifiable Information for longer than 90 days following completion of the SELLER's services for the BRAND program (unless otherwise required by law).
   6.4. Data Storage: Securely store and protect all physical and electronic personal identifiable information to prevent accessibility to unauthorized personnel including but not limited to: hard drives, laptops, computers, cell phones, and paper files.

7. Data /File Transfer:
   7.1. Cross Border Transfer: Personally Identifiable Information collected for use with a BRAND program may only be held and processed in the United States or in the jurisdiction where the data subject resides. Any need to transfer Personally Identifiable Information to other jurisdictions must first be consented to by PEP and the BRAND in writing. If it is necessary to transfer data about a data subject that is located anywhere in the European Economic Area ("EEA") from the EEA to the United States or to another jurisdiction that has not been approved by the European Commission as providing adequate data protection safeguards, SELLER shall confirm to PEP whether it is in possession of a valid EU-US Privacy Shield certification. To the extent that the EU-US Privacy Shield transfer mechanism is declared invalid by a court of relevant authority of a competent jurisdiction, or if SELLER ceases to be EU-US Privacy Shield certified, and SELLER continues to have a need to transfer personal data outside the EEA, SELLER agrees to immediately notify PEP and PEP and SELLER agree to enter into the Standard Contractual Clauses set forth at https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en.
   7.2. EU General Data Protection Regulation: For purposes of the EU General Data Protection Regulation 2016/679 ("GDPR") and the data privacy laws of EU jurisdictions subject to the GDPR ("EU Data Protection Laws"), SELLER and PEP are each considered a data processor of the

Personally Identifiable Information that it collects and the BRAND is the data controller. Where necessary to comply with EU Data Protections Laws, SELLER agrees to cooperate with PEP and the BRAND and to promptly complete any related contractual and/or administrative requirements, including without limitation a Data Protection Addendum to the Agreement. All such agreements shall be incorporated by reference herein.

7.3. Personally Identifiable Information: Use PEP-approved industry standard encryption or pseudonymization methods when collecting and transferring Personally Identifiable Information as more fully described in the Security Requirements section.

7.4. File Transfer: Use secure file transfer protocols (at a minimum, industry standard protocols) when transferring data files. Ensure reasonable security measures are in place for physically transferring electronic and hard copy personally identifiable information.

7.5. File Receipt: Limit the number of people that data files are sent to.

8. Children:

8.1. Do not Collect: Do not collect Personally Identifiable Information online from individuals under the age of 16 in connection with any BRAND program without the prior written authorization of PEP. Do not provide PEP with Personally Identifiable Information collected online from individuals under the age of 16.

8.2. Age/State Check: Verify that websites and other online programs used in connection with the BRAND programs do not collect Personally Identifiable Information from individuals under the age of 16 by asking for month and year of birth before collecting Personally Identifiable Information. This includes mobile programs. All age screening methods must comply with applicable guidelines of the Children's Advertising Unit of the Better Business Bureau ("CARU"). Consult your PEP contact for appropriate wording for age checking and other requirements.

8.3. Minimal Collection: Where you have received written authorization from PEP for collecting Personally Identifiable Information from children, ask only for the minimum information necessary for a child to participate in the BRAND program.

8.4. Parental Access: Where you have received written authorization from PEP for collecting Personally Identifiable Information from children, confirm that the process used to collect such information conforms to the requirements of the Children's Online Privacy Protection Act and the applicable FTC regulations, as well as CARU.

9. Protected Health Information:

9.1. If SELLER collects or has access to "protected health information" (as that term is defined in the HIPAA Privacy Rule), then SELLER will notify PEP and enter into a Business Associate Agreement, in form that meets the minimum HIPAA requirements and is acceptable to PEP and the BRAND.

10. Accountability:

10.1. Management Commitment: Establish and demonstrate top management's commitment to maintaining the trust placed in the BRAND(s) and PEP by those who give Personally

Identifiable Information by following PEP's Requirements and implementing appropriate privacy and security.

10.2. Privacy Responsibility: Appoint an individual with the responsibility to oversee and to coordinate the information privacy arrangements in business units/departments. This individual should have enterprise-wide responsibility for verifying that PEP's Requirements are implemented.

10.3. Privacy Training and Awareness: At least once per year, 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 these Privacy Requirements. In addition, SELLER shall conduct annual training of all its employees and SELLER'S REPRESENTATIVES' employees with access to BRAND Information concerning the BRAND's Privacy and Security Requirements.

10.4. Privacy Compliance: Procedures must be in place to confirm that services provided to and operations of BRAND programs are compliant with these Privacy Requirements before they go into production. Monitor programs and systems to ensure that Personally Identifiable Information, HRI and Brand Information is secure, protected and used appropriately.

10.5. Privacy Incidents: Adopt a formal data breach response program which includes the following elements: (1) notification of PEP as soon as possible but no later than 24 hours after discovery of an actual or suspected breach of the security of its system or unauthorized access to Personally Identifiable Information (a "Breach"); (2) prompt remedial measures to address the source and cause of the Breach at SELLER's own cost; (3) reasonable actions to mitigate any harm caused by the Breach at SELLER's own cost; (4) regular communication with PEP and cooperation with PEP and the BRAND with respect to its investigation and to provide PEP with any requested information relative to the Breach. SELLER agrees to obtain PEP's prior written consent before notifying any third parties of the Breach, including law enforcement, regulatory agencies, or impacted individuals; provided that SELLER may inform, at its own discretion, other entities directly impacted by the underlying incident causing the Breach and any Breach response professionals, provided that SELLER shall not be permitted to reference the BRAND in such communication.

10.6. Subcontractors: SELLER and/or SELLER's REPRESENTATIVES must have PEP's prior written consent before providing any subcontractor any Personally Identifiable Information collected on behalf of a BRAND. Use of subcontractors is subject to the requirements of Section 31.3 of PEP's Security Requirements and Section 27 of the Agreement.

10.7. Self-Assessment: Upon reasonable notice, SELLER's and/or SELLER's REPRESENTATIVES handling Personally Identifiable Information must complete PEP's vendor information privacy assessment to ensure compliance with these Privacy Requirements.

11. Additional Terms for Online Collection, Maintenance, and Use of Data. If SELLER, as part of providing goods or services under the Agreement, hosts any web-based content or other digital content on behalf of PEP or a BRAND on any server not owned or controlled by PEP, then the

additional terms in this Section 11 apply. Further, SELLER acknowledges that under no circumstances will it use Tracking Technologies (as defined below) in connection with the collection of data from Users (as defined below) who reside in the European Economic Area without PEP's prior written consent.

11.1. Definitions.

11.1.1. "Applicable Self-Regulatory Principles" means industry accepted self-regulatory principles governing Behavioral Data Services, including the Self-Regulatory Principles for Online Behavioral Advertising, available at www.aboutads.info and the Network Advertising Initiative's Code of Conduct, available at www.networkadvertising.org.

11.1.2. "Brand Property(ies)" means any website, micro-site, app or other electronic or digital property owned or controlled by the BRAND, that includes any goods or services offered by the BRAND, and/or that includes BRAND trademarks, logos, or other PEP IP.

11.1.3. "Brand Data" means any and all User Data and/or other non-Personally Identifiable Information (i) provided by or on behalf of PEP and/or BRAND to SELLER that is not; or (ii) collected in connection with the performance of the services or provision of the goods to PEP and/or the Brand.

11.1.4. "Online Behavioral Advertising" has the meaning set forth in all Applicable Self-Regulatory Principles.

11.1.5. "Tracking Technology(ies)" is defined in Section 11.2.

11.1.6. "User" means any visitor to a Brand Property via a computer, other device (e.g., mobile telephone), automated process, or software.

11.1.7. "User Data" means any Brand Data that is non-Personally Identifiable Information that can be attributed to a User or a User's computer or device, in any medium or format, including, without limitation, cookies, IP addresses, or any other identifiers, and data about a User's computer or device collected via use of any Tracking Technology that identifies the User or the User's online activity (e.g., details of pages, objects or other content that a User has clicked on, the content viewed by the User, searches conducted by the User, the User's response to campaign ads, etc.).

11.2. Use of Tracking Technology(ies). In providing the services, SELLER will only use methods of operation and data collection capabilities for any cookie, Javascript, Pixel, beacon, statistical ID, probabilistic ID, UDID, or similar tracking mechanism or other method of monitoring a user or device across web and/or app locations or properties ("Tracking Technology(ies)") whose methods of operation and data collection capabilities have been fully disclosed to PEP and approved in writing, consistent with Attachment A attached to these Privacy Requirements, and/or have been expressly requested by PEP. Under no circumstances will SELLER use: (i) Flash local shared objects, (ii) Tracking Technologies for online behavioral advertising purposes; (iii) Tracking Technologies that are or can be used to circumvent the preferences and/or options selected by a User as to Tracking Technologies, as provided in web browser privacy controls or other software used by the user; (iv) any Tracking Technologies that are not publicly known or that fail to provide Users with an opportunity to control the use of such Tracking Technologies;

(v) Tracking Technologies that collect user data across different Brand Properties, whether for advertising or other purposes; (vi) Tracking Technologies deployed on behalf of other parties (so-called "fourth-party" tracking or "piggybacking") for online behavioral advertising or other purposes; or (vii) Tracking Technologies to collect, disclose, process, transmit or otherwise use any PII.

11.3. Brand Data. SELLER shall: (i) not collect, process, store, disclose, dispose or otherwise use any Brand Data or User Data in any manner not required to provide the Goods/Services; (ii) contractually require any third party to which Brand Data and/or User Data is provided to abide by the use restrictions set forth in the Addendum and Agreement; (iii) not seek to re-create, reverse engineer or re-identify any Brand Data and/or otherwise associate such Brand Data with any PII; (iv) permit PEP to block and/or remove any Tracking Technology from any Brand Property at any time without any additional approval from SELLER. SELLER may, upon written notice to PEP, suspend performance of the Goods/Services if (i) PEP blocks, removes, or manipulates SELLER's Tracking Technology and (ii) such action by PEP makes SELLER unable to deliver the Goods/Services – in such case, the parties shall promptly meet to discuss how to resolve SELLER's suspension.

11.4. Representations & Warranties. SELLER represents and warrants that: (i) SELLER will at all times maintain and provide to PEP an up-to-date list of any current investigations by any regulatory agency, legislative body, and/or any pending litigation, disputes, and/or threats related to the provision of Goods/Services; (ii) SELLER will not, directly or indirectly, introduce to any Brand Property or to the computer or any other device of any User, any virus, worm, Trojan horse, spyware, or other form of malware; (iii) SELLER has not been and shall not be, in connection with the development of the computer code underlying the Goods/Services, negligent in terms of the removal of any vulnerabilities in such computer code that would permit unauthorized access, including without limitation, any unauthorized access that would permit the introduction of any of the types of malware listed in section 4(ii); and (iv) SELLER and any subcontractor or other person or entity acting on its behalf will comply with all applicable data privacy-related laws, regulations and professional requirements triggered by the services provided to PEP under the Agreement. SELLER WILL IMMEDIATELY INFORM PEP IN WRITING OF ANY BREACH OF THE REPRESENTATIONS AND/OR WARRANTIES MADE IN THESE REQUIREMENTS. FAILURE TO PROVIDE NOTICE TO PEP SHALL BE CONSIDERED A MATERIAL BREACH OF THE AGREEMENT.

11.5. Ownership. All right, title, and interest in and to any Brand Data will be solely owned by PEP and/or the BRAND. For the avoidance of doubt, except for the as provided herein, SELLER may not edit, modify, create derivative works from, re-identify, create combinations or compilations of, combine, associate, synthesize, reproduce, license, sublicense, display, distribute, disclose, process or otherwise use any Brand Data.

11.6. Record Retention and Disposal. SELLER will maintain a records retention process and a business continuity plan for all Brand Data in SELLER's control or custody. SELLER will destroy Brand Data using a secure means of disposal (e.g. incineration or cross-cut shredding) when such data

is no longer required and under no circumstances retain Personally Identifiable Information for longer than 90 days following completion of the SELLER's services for the BRAND program (unless otherwise required by law). Hardware containing Brand Data must be physically destroyed or securely overwritten prior to disposal or use for another purpose.

11.7. Termination of Agreement. Upon completion of the services and/or voluntary or involuntary termination of the Agreement, upon request, SELLER agrees to promptly return all Brand Data collected in connection with the Agreement to PEP and in SELLER's control or custody.

PEP'S SECURITY REQUIREMENTS

PEP's security methodology is based on 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 SELLERs who collect, use, transfer or store Personally Identifiable Information. Before the SELLER may collect, use, transfer or store Personally Identifiable Information under the Agreement they must have a valid contract, statement of work, or purchase order with the privacy and security language in place.

The guidelines described below are comprehensive in nature, and each SELLER 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:

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

12. Information Security Governance
    12.1. Management Commitment: Top management's direction on information security should be established, and commitment demonstrated.
    12.2. Information Security Function: An information security function should be established, which has enterprise-wide responsibility for promoting information security.
    12.3. Local Security Co-ordination: An individual should be appointed to co-ordinate the information security arrangements in business units/departments.
    12.4. Security Audit / Review: The information security status should be subject to thorough, independent and regular security audits/reviews. SELLER grants PEP the right to conduct an audit no more than once per year until the initial audit identifies a material audit finding (in which case PEP is entitled to audit the non-compliant controls until such material finding is

remediated). SELLER agrees to cooperate with the audit by providing access to knowledgeable personnel, premises, systems/networks, policies, standards, documentation, and where possible, those same elements for SELLER's subcontractors used to provide services to or on behalf of the BRAND. SELLER is not obligated to disclose or make available any systems or information that is confidential third-party information. At its cost, SELLER will promptly remediate any audit findings, and to the extent SELLER disagrees with such finding, work in good faith to negotiate a mutually satisfactory mitigation strategy. To the extent that PEP and SELLER cannot reach agreement on a mitigation strategy for a material audit finding, BUYER will have the right to terminate the Agreement for convenience with thirty (30) days prior written notice without any penalty, liability or further obligation. As an alternative, PEP may choose to accept an independent verification (e.g. SOC 2 Type II) of SELLER's compliance with these Security Requirements.

12.5. Security Monitoring: The information security condition of the enterprise should be monitored periodically and reported to top management.

13. Information Security Policy
    13.1. 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. Such policy should be reviewed and communicated to all applicable individuals on at least an annual basis.
    13.2. Security Architecture: An information security architecture should be established, which provides a framework for the application of standard security controls throughout the enterprise.
    13.3. Certification: Provide to PEP upon request written certification of compliance to the Massachusetts Code of Regulations, 201 CMR §§ 17.00 et. seq., as applicable.

14. Security Education / Awareness
    14.1. Security Awareness: Employees should be made aware of the key elements of information security, why it is needed, and understand their Personally Identifiable 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.
    14.2. Security Education: Staff should be educated/trained in how to run systems correctly and how to develop and apply security controls.

15. Accountability / Ownership
    15.1. 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. Criminal background checks must be performed where

permitted by law, and results considered, prior to staff being assigned any information security responsibilities.

15.2. 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.

16. Information Risk Analysis

16.1. Risk Analysis: Critical applications, computer installations, networks and systems should be subject to a formal risk analysis on a periodic basis, which shall include testing, assessing and evaluating their effectiveness. The results should be documented, reviewed, and approved by the appropriate owner. Identify material internal and external risks to the security, confidentiality, and integrity of personal information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction or other compromise of such information, and assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, the risk analysis should include consideration of risks in each area of relevant operation including but not limited to:

16.1.1. Employee training and management;

16.1.2. Information systems, including network and software design, information processing, storage, transmission, and disposal;

16.1.3. Prevention, detection, and response to attacks, intrusions, or other systems failures;

16.1.4. Design and implement reasonable safeguards to control the risks identified through the analysis and conduct regular testing or monitoring of the effectiveness of the safeguards' key controls, systems and procedures.

16.2. Confidentiality Requirements: The impact of business information stored in or processed by the application being disclosed to unauthorized individuals should be assessed.

16.3. Integrity Requirements: The impact of business information stored in or processed by the application being accidentally corrupted or deliberately manipulated should be assessed.

16.4. Availability Requirements: The impact of business information stored in or processed by the application being unavailable for any length of time should be assessed.

17. Asset Management

17.1. 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.

17.2. 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.

17.3. Device Management: SELLER will use only securely configured, corporate-owned devices (i.e. non BYOD or hybrid/work personal use devices) to connect to BRAND networks and systems or to access or store Personally Identifiable Information, HRI or Brand Information.

17.4. Handling Information: Additional protection is provided for handling Personally Identifiable Information, HRI, and Brand Information. Two-factor authentication of SELLER and SELLER'S REPRESENTATIVE'S administrators, users and/or authorized subcontractors is required when providing access to Personally Identifiable Information online. Files containing Personally Identifiable Information or Protected Health Information subject to HIPAA are required to be transferred via secure file transfer protocols using encryption for data in transit and at rest, consistent with industry standard encryption methods. SELLER and SELLER'S REPRESENTATIVE's must not store any Personally Identifiable Information, HRI or Brand Information on any portable device or media (e.g., laptop, flash drive, Smartphone) that does not utilize industry standard, full disk (where possible) encryption. Personally Identifiable Information, HRI or Brand Information must be encrypted when in transit and at rest consistent with accepted industry encryption standards.

17.5. Acquisition: Robust, reliable hardware and software should be acquired following consideration of security requirements and identification of any security deficiencies.

18. Identity and Access Management

18.1. Access Control: Access to the application and associated information should be restricted to authorized individuals and enforced accordingly. SELLER will maintain a process that both monitors and enforces access rights to BRAND systems and Personally Identifiable Information. Wireless access to BRAND networks and systems must be via secure connections (i.e. VPN) and over private wireless routers. Upon request by BRAND or PEP, SELLER will execute a non-disclosure agreement.

18.2. User Authorization: All users of the computer installation should be authorized before they are granted access privileges.

18.3. User Authentication: All users should be authenticated by using User IDs 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. Two-factor authentication of SELLER and SELLER'S REPRESENTATIVE'S administrators, users and/or authorized subcontractors is required when providing access to BRAND Information online (e.g., system or data base level administrative access) to any servers and/or application hosting BRAND Information), or by use of remote access. Require strong password authentication commensurate with the type of data being collected. Require strong and unique passwords with a combination of letters, uppercase, numbers, symbols. Do not allow common dictionary passwords to be used such as "password" or "12345". Store user passwords and reset/forgotten security questions in an encrypted manner.

18.4. Sign-on Process: Users should follow a rigorous system sign-on process before they can gain access to target systems. Log-in processes should be disabled after multiple (consecutive) access attempts are made.

19. Application and Services Security

19.1. Resilience: The applications, computer installations and networks should be run on robust, reliable hardware and software, supported by alternative or duplicate facilities.

19.2. Back-up: Back-ups of essential information and software should be taken on a regular basis and to an offsite location, on a minimum of a daily basis, according to a defined cycle.

19.3. Web-enabled Applications: All internet facing websites accessed by BRAND or PEP employees or consumers must have industry standard tuned Web Application Firewall (WAF). Specialized technical controls should be applied to web-enabled applications to ensure that the increased risks associated with web-enabled applications are minimized. All internet facing websites accessed by BRAND employees or consumers must be scanned and remediated using accepted industry standard for security vulnerabilities (e.g., Open Web Application Security Project, and Open Web Application Security Project Top 10, etc.). Scans and remediation must first be completed prior to application launch. Post launch, SELLER will conduct scans at a frequency that is appropriate for the relevant application, technology and data risk. Websites will implement and maintain accepted industry standard account and password management controls, including:

19.3.1. Lockout after no more than ten unsuccessful login attempts;

19.3.2. Prohibiting user IDs, passwords and PII from being displayed in a URL;

19.3.3. Storing user passwords and reset/forgotten security questions in an encrypted manner;

19.3.4. Re-authentication is required after no more than 30 minutes of inactivity;

19.3.5. Prohibiting the storage of passwords or PII in persistent local storage (caches, etc.) or in any cookies, Javascript, or other web tracking technology;

19.3.6. All users should be authenticated by using User IDs 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. Two-factor authentication of SELLER and SELLER'S REPRESENTATIVE'S administrators, users and/or authorized subcontractors is required when providing access to information online;

19.3.7. Require strong and unique passwords with a combination of letters, uppercase, numbers, and symbols;

19.3.8. Do not allow common dictionary passwords to be used such as "password" or "12345".

19.4. Ecommerce: A process should be established to ensure that information security is incorporated into electronic commerce initiatives enterprise-wide.

19.5. PCI Compliant: To the extent SELLER has access to cardholder payment card information including, but not limited to, account number, expiration date, or 3 digit code, SELLER represents and warrants that it is a Level 1 PCI Compliant Merchant or Service Provider, as applicable, as defined at https://usa.visa.com/support/small-business/security-compliance.html#2. SELLER will furnish evidence of its PCI-DSS compliance upon request by PEP, by having its PCI scope assessed by a Qualified Security Assessor (QSA) with an annual Report of Compliance. SELLER is responsible for the security of BRAND cardholder data that SELLER possesses or otherwise stores, processes, or transmits on behalf of BRAND and will furnish evidence of current PCI-DSS certification for the relevant services. SELLER will conduct PCI -DSS required quarterly network scans on the in-scope environment via an Approved Scanning Vendor (as defined by PCI-DSS).

19.6. General Security Controls: The full range of general security controls should be considered when designing systems and services.

19.7. Application Controls: The full range of application and systems controls should be considered, and required controls identified.

20. Physical and Environmental Security

20.1. 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.

20.2. Hazard Protection: Computer equipment and facilities should be protected against fire, flood, environmental and other natural hazards.

21. System Configuration

21.1. Host System Configuration: Host systems should be configured to function as required, and to prevent unauthorized or incorrect updates.

21.2. 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.

21.3. Configuration of Network: Network devices should be securely configured to function as required, and to prevent unauthorized or incorrect updates.

21.4. 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.

22. System Monitoring

22.1. Event Logging: SELLER must have a documented log review process. Administrators with privileged access to BRAND Information must not be allowed to perform log maintenance. Logs of all key events within the computer installation should be maintained (preferably using

automated tools), reviewed periodically and protected against unauthorized change. The following logs must be captured and actively monitored:

22.1.1. Successful and failed logins of users and administrators;

22.1.2. All admin access to the BRAND Information and systems provided as part of the Services;

22.1.3. Changes to security configuration settings (password requirements, encryption settings, etc.);

22.1.4. Other security relevant events (database transaction logging, database access logging, etc.).

22.2. System Network Monitoring: Systems associated with the computer installation should be monitored continuously, and from a business user's perspective.

22.3. Intrusion Detection and Penetration Testing: Intrusion detection mechanisms should be applied to critical systems and networks. SELLER will perform or contract to perform ethical penetration testing of the environment on an at least annual basis with remediation and patching of discovered vulnerabilities.

23. Network Security

23.1. 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.

23.2. Network Documentation: Networks should be supported by accurate, up-to-date documentation.

23.3. External Access / Connections: All external connections to the network should be individually identified, verified, recorded, and approved by the network owner.

23.4. Firewalls: Network traffic should be routed through a firewall, prior to being allowed access to the network.

23.5. Wireless Access: Wireless access should be authorized, authenticated, encrypted and permitted only from approved locations.

24. Electronic Communication

24.1. Special Voice Network Controls: Voice network facilities (ex: telephone exchanges) should be monitored regularly and access to them restricted.

24.2. Email: E-mail systems should be protected by a combination of policy, awareness, procedural and technical security controls.

24.3. Instant Messaging: Instant Messaging systems should be protected by a combination of policy, awareness, procedural and technical security controls.

25. Cryptography

25.1. Cryptography: Cryptographic solutions should be approved, documented and applied enterprise-wide.

25.2. 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.

25.3. Encryption: Utilize industry-tested and industry-accepted methods of encryption and pseudonymization when collecting, storing, and transferring personally identifiable information.

26. Information Privacy

26.1. Information Privacy: Responsibility for managing information privacy should be established and security controls for handling personally identifiable information applied.

26.2. Alignment with PEP Privacy: Personally Identifiable Information is collected, used, stored, transferred, and destroyed according to PEP privacy guidelines. Refer to the PEP Data Privacy Requirements section of these Privacy Requirements for details on use and collection of Personally Identifiable Information

27. Malware Protection

27.1. Virus Protection: Virus protection arrangements should be established, and maintained enterprise-wide.

27.2. Malicious Code Protection: Enterprise-wide arrangements should be established to protect against malicious code, such as that downloaded from the web.

28. System Development

28.1. 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.

28.2. Quality Assurance: Quality assurance of key security activities should be performed during the development lifecycle.

28.3. Specification of Requirements: Business requirements (including those for information security) should be documented and agreed before detailed design commences.

28.4. 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.

28.5. Testing: All elements of a system (ex: application software packages, system software, hardware and services) should be tested before the system is promoted to the live environment.

28.6. System Promotion Criteria: Rigorous criteria should be met before new systems are promoted into the live environment.

28.7. Installation Process: New systems should be installed in the live environment in accordance with a documented installation process.
28.8. Post-implementation Review: Post-implementation reviews should be conducted for all new systems.

29. Change Management
29.1. 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.
29.2. Change Management: Changes to any part of the computer installation should be tested, reviewed and applied using a change management process.
29.3. Patch Management: There is a strategy for patch management and a documented patch management process, including ensuring that updates and patches to third party software are implemented in a timely manner.
29.4. Remote Maintenance: Remote maintenance of the network should be restricted to authorized individuals, confined to individual sessions, and subject to review.
29.5. Security Warnings: Implement processes for receiving and addressing reports about security vulnerabilities in a timely manner

30. Incident Management
30.1. Incident Management: All incidents – of any type – should be recorded, reviewed and resolved using an incident management process.
30.2. Alignment with PEP Privacy: Incidents are reported to PEP immediately (in all instances, within 24 hours).
30.3. Forensic Investigations: A process should be established for dealing with incidents that require forensic investigation.

31. Third Party Management
31.1. 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.
31.2. 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.
31.3. 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 (such requirements to be no less rigorous than the applicable terms of these Privacy Requirements).

31.4. Hosted Systems/Use of Cloud Services. SELLER will notify PEP in writing when it hosts Personally Identifiable Information or Highly Restricted Information in a shared or cloud environment. SELLER will protect (or cause its Subcontractor to protect) the Personally Identifiable Information or Highly Restricted Information hosted in a cloud environment using controls consistent with accepted industry standards (e.g., Cloud Security Alliance Cloud Controls Matrix). SELLER will collaborate in good faith to identify an alternative to such hosting should PEP or the BRAND so request.

32. Business Continuity
    32.1. Business Continuity: A business continuity plan should be developed, supported by contingency arrangements, and tested annually.
    32.2. Power Supplies: Critical computer equipment and facilities should be protected against power outages.

33. PEP Director of Information Security. All inquiries and questions concerning the Security Requirements should be directed to the PEP Privacy & Governance Lead by calling 513-826-0101.

Last updated 4/10/2019

TPG Rewards, Inc. Privacy Policy

Privacy Notice

UPDATED AS OF: February 1, 2018

TPG Rewards, Inc. is committed to maintaining your confidence and trust as it relates to the privacy of your information. Please read below and learn how we collect, protect, share and use your information during your participation in any of our promotions and when you visit our technology platforms, including, without limitation, our websites, interactive features, applications, social network pages, and mobile application ("Platforms").

1. INFORMATION COLLECTED ON OUR PLATFORMS.

Information You Provide To Us

We may collect Personal Information (information that can be used to identify you as an individual) such as your name, email, telephone number, home address, demographic information (such as zip code, age), or payment information (such as account or credit card number). The types of Personal Information we collect may vary depending on your use of the features of the Platforms. In many cases we need this information to provide the personalized or enhanced service that you are interested in. You never have to answer our questions regarding your Personal Information, and you can decline this exchange of information on any site on the Internet - not just ours - at any time.

Information Collected Automatically

Usage Information. Whenever you participate in one of our programs or visit or interact with the Platforms, we, as well as any third-party advertisers and/or service providers, may use a variety of technologies that automatically or passively collect information about how the programs or Platforms are accessed and used ("Usage Information"). Usage Information may include browser type, device type, operating system, application version, the page served, the time, the preceding page views, and your use of features or applications on the Platforms, interaction with

friends and group activities, information derived from receipts, purchasing trends and online and offline activities and interests. This information helps us keep our programs and Platforms fresh and interesting to our visitors and allows us to tailor content to a visitor's interests. We may also anonymize or group this information into aggregate visitor data in order to describe the use of the Platforms or promotion to our existing or potential business partners, sponsors or other third parties.

Device Identifier. We automatically collect your IP address or other unique identifier ("Device Identifier") for the Device (computer, mobile phone, tablet or other device) you use to access the promotions or Platforms. A Device Identifier is a number that is assigned to your Device when you access a website or its servers, and our computers identify your Device by its Device Identifier. We may use a Device Identifier to, among other things, administer the Platforms, help diagnose problems with our servers, analyze trends, track users' web page movements, help identify you and your promotion entry, and gather broad demographic information for aggregate use.

Cookies; Pixel Tags. The technologies used in our promotions and on the Platforms to collect Usage Information, including Device Identifiers, include but are not limited to: cookies (data files placed on a Device when it is used to visit the Platforms), mobile analytics software and pixel tags (transparent graphic image, sometimes called a web beacon or tracking beacon, placed on a web page or in an email, which indicates that a page or email has been viewed). Cookies may also be used to associate you with social networking sites like Facebook and Twitter and, if you so choose, enable interaction between your activities on the Platforms and your activities on such social networking sites We, or our vendors, may place cookies or similar files on your Device for security purposes, to facilitate site navigation and to personalize your experience while visiting our Platforms (such as allowing us to select which ads or offers are most likely to appeal to you, based on your interests, preferences, location, or demographic information). A pixel tag may tell your browser to get content from another server.

To learn how you may be able to reduce the number of cookies you receive from us, or delete cookies that have already been installed in your browser's cookie folder, please refer to your browser's help menu or other instructions related to your browser. If you do disable or opt-out of receiving cookies, please be aware that some features and services on our Platforms may not work properly because we may not be able to recognize and associate you with your TPG Rewards account(s). In addition, the offers we provide when you visit us may not be as relevant to you or tailored to your interests.

2. HOW WE USE THE INFORMATION WE COLLECT.

We use the information we collect about and from you for a variety of business purposes such as to respond to your questions and requests; provide you with access to certain areas and features of the Platforms or programs and your interaction with other users; verify your identity; communicate with you about your account and activities on the Platforms and, in our discretion, changes to any TPG Rewards policy; tailor content, advertisements, and offers we or our business partners may serve you; improve the Platforms; comply with license obligations; and for purposes disclosed at the time you provide your Personal Information or otherwise with your consent. We may also collect your location-based information for the purpose of providing you with certain services.

3. SHARING OF INFORMATION.

Except as described in this Privacy Notice, we will not provide any of your Personal Information to any third parties without your consent. We may share non-Personal Information, such as aggregate data and Usage Information with third parties. We may also share your information as disclosed at the time you provide your information, as set forth in this Privacy Notice and in the following circumstances:

Third Parties Providing Services On Our Behalf. We create promotions with consumer product companies who sponsor the offers that we provide to you. We may share your Personal Information and Usage Information with such consumer product companies and also third parties that perform functions on our behalf (or on behalf of our partners) such as service providers that host or operate our Platforms, analyze data, process transactions and payments, or provide customer service; advertisers; sponsors or other third parties that participate in or administer our promotions, contests, sweepstakes, surveys or provide marketing or promotional assistance and "powered by"

partners or partners in co-branded sites. Your Personal Information may also be used by us or shared with our subsidiaries, affiliates, sponsors, partners, advertisers or other third parties to provide you with product information and promotional and other offers.

Your Agreement To Have Your Personal Information Shared. While on our Platforms, you may have the opportunity to opt-in to receive information and/or marketing offers from someone else or to otherwise consent to the sharing of your information with a third party, including social networking sites such as Facebook or Twitter. If you agree to have your Personal Information shared, your Personal Information will be disclosed to the third party and the Personal Information you disclose will be subject to the privacy policy and business practices of that third party.

Business Transfers. We may share your Personal Information with other entities and our affiliates primarily for business and operational purposes. In the event that TPG Rewards is involved in a bankruptcy, merger, acquisition, reorganization or sale of assets, your information may be sold or transferred as part of that transaction.

Legal Disclosure. We may transfer and disclose your information to third parties to comply with a legal obligation; when we believe in good faith that the law or a governmental authority requires it; to verify or enforce our Terms of Use or other applicable policies; to address fraud, security or technical issues; to respond to an emergency; or otherwise to protect our rights or property or security of third parties, visitors to our Platforms or the public.

4. INFORMATION WE RECEIVE FROM THIRD PARTIES.

We may receive information about you from third parties. For example, if you are on another website and you opt-in to receive information from TPG Rewards, that website will submit to us your email address and other information about you so that we may contact you as requested. You may also choose to participate in a third party application or feature (such as one of our Facebook or Twitter applications or a similar application or feature on a third party website) through which you allow us to collect (or the third party to share) information about you, including Usage Information and Personal Information such as lists of your friends, "likes", comments you have shared, groups and location. Services like Facebook Connect may give you the option to post information about your activities on our Platform to your profile page to share with others within your network. In addition, we may receive information about you if other users of a third party website give us access to their profiles and you are one of their "connections" or information about you is otherwise accessible through your "connections'" web page, profile page, or similar page on a social networking or other third party website or interactive service. We may supplement the information we collect about you through the Platforms with such information from third parties in order to enhance our ability to serve you, to tailor our content to you and/or to offer you opportunities to purchase products or services that we believe may be of interest to you.

5. YOUR PRIVACY RIGHTS, CHOICE AND ACCESS.

You may always direct us not to share your Personal Information with third parties, not to use your Personal Information to provide you with information or offers, or not to send you newsletters, emails or other communications by: (i) modifying your registered user information on the Platforms; (ii) sending us an email at customerservice@tpgny.com; (iii) contacting us by mail at TPG Rewards Inc, 29 Broadway, Ste 1400, New York, NY 10006; or (iv) following the removal instructions in the communication that you receive. Your opt-out request will be processed within 30 days of the date on which we receive it.

If you wish to modify, verify, correct, or delete any of your Personal Information collected through the Platforms, you may edit your registered user information or contact us at the above address or email. In accordance with our routine record keeping, we may delete certain records that contain Personal Information you have submitted through the Platforms. We are under no obligation to store such Personal Information indefinitely and disclaim any liability arising out of, or related to, the destruction of such Personal Information. It may not always possible to completely remove or delete all of your information from our databases without some residual data because of backups and other reasons. We will retain your information (including geo-location data) for as long as your account is active or as needed to provide you services. If you wish to cancel your account or request that we no longer use your

information to provide you services contact us a customerservice@tpgny.com. We will retain and use your information as necessary to comply with our legal obligations, resolve disputes, and enforce our agreements. We do not control certain privacy settings and preferences maintained by our social media partners like Facebook and Twitter. If you wish to make changes to those settings and preferences, you may do so by visiting the settings page of the appropriate social media site.

6. ADVERTISING/BEHAVIORAL TARGETING; HOW TO OPT-OUT.

We may use third party ad network providers to help present ads on the Platforms, as well as other service providers to evaluate and provide us with information about the use of the Platforms and viewing of our content. We do not share Personal Information with these providers (unless, of course, you give us permission). Such providers may place and access cookies, pixel tags, or similar technologies on your Device to serve you ads or other content personalized to your interests which they infer from your browsing on the Platforms and other sites you have visited. In doing so, the provider collects or has access to non-Personal Information such as your Usage Information. The use of cookies, pixel tags, or similar technologies by these providers is subject to their own privacy policies, not ours.

If you do not want to receive the benefits of targeted advertising, you may opt-out of some network advertising programs that use your information by visiting the NAI Opt-Out Page at http://www.networkadvertising.org/managing/opt_out.asp. Please note that even if you choose to remove your information (opt-out), you will still see advertisements while you're browsing online. However, the advertisements you see may be less relevant to you and your interests. Additionally, many network advertising programs allow you to view and manage the interest categories they have compiled from your online browsing activities. These interest categories help determine the types of targeted advertisements you may receive. The NAI Opt-Out Page provides a tool that identifies its member companies that have cookies on your browser and provides a mechanism to opt-out of receiving cookies from those companies.

7. CHILDREN.

We do not knowingly collect, use or disclose personally identifiable information from anyone under 13 years of age. If we determine upon collection that a user is under this age, we will not use or maintain his/her Personal Information without the parent/guardian's consent. If we become aware that we have unknowingly collected personally identifiable information from a child under the age of 13, we will make reasonable efforts to delete such information from our records.

8. SECURITY OF YOUR INFORMATION.

We take information security seriously and use certain reasonable security measures to help protect your Personal Information. However, no electronic data transmission or storage of information can be guaranteed to be 100% secure. Please note that we cannot ensure or warrant the security of any information you transmit to us, and you use the Platforms and provide us with your information at your own risk.

9. OTHER SITES.

The Platforms may contain links to other sites that we do not own or operate. This includes links from advertisers, sponsors and/or partners that may use our logo(s) as part of a co-branding or co-marketing agreement. We do not control, recommend or endorse and are not responsible for these sites or their content, products, services or privacy policies or practices. These other sites may send their own cookies to your Device, they may independently collect data or solicit Personal Information and may or may not have their own published privacy policies. You should also independently assess the authenticity of any site which appears or claims that it is one of our Platforms (including those linked to through an email or social networking page).

The Platforms may make available chat rooms, forums, message boards, and news groups. Remember that any information that you disclose in these areas becomes public information and is not subject to the provisions of this Privacy Notice.

10. CONSENT TO PROCESSING AND TRANSFER OF INFORMATION.

The Platforms are governed by and operated in, and in accordance with the laws of, the United States. TPG Rewards makes no representation that the Platforms are governed by or operated in accordance with the laws of any other nation. Given that we are an international business, our use of your information necessarily involves the transmission of data on an international basis. If you are located in the European Union, Canada or elsewhere outside of the United States, please be aware that information we collect may be transferred to and processed in the United States. By using the Platforms, or providing us with any information, you (a) acknowledge that the Platforms are subject to the laws of the United States, (b) consent to the collection, processing, maintenance and transfer of such information in and to the United States and other applicable territories in which the privacy laws may not be as comprehensive as or equivalent to those in the country where you reside and/or are a citizen, and (c) waive any claims that may arise under those laws.

11. CHANGES.

We may update this Privacy Notice to reflect changes to our information practices. If we make any material changes we will notify you by email (sent to the e-mail address specified in your account) or by means of a notice on our Platforms prior to the change becoming effective. We encourage you to periodically review this page for the latest information on our privacy practices.

12. CONTACT US.

If you have any questions or concerns about this Privacy Notice, the practices of the Platforms, or your experiences with the Platforms, please contact us at:

TPG Rewards Inc., 29 Broadway, Ste 1400, New York, NY 10006, (800) 838-4550 Email: Customerservice@tpgny.com