

[See Our Privacy Policy | Sago](#)

<https://sago.com/en/legal/privacy/>

PRIVACY POLICY

Updated 11 December 2023

1.1. Purpose

Privacy policy of SS Holdings Group, LLC D/B/A Sago, branded as “Sago”, for people who are engaging with us or our digital platforms as research or prospective clients, as research partners or participants (e.g., consumers, healthcare professionals, patients, or business individuals).

1.2. Policy

Your privacy is important to us.

It is Sago’s policy to respect your privacy and comply with any applicable law and regulation regarding any personal information we may collect about you, including across our website, and other sites we own and operate.

In the event our site contains links to third-party sites and services, please be aware that we have no control over the content and policies of those sites and cannot accept responsibility or liability for their respective privacy practices.

Our privacy policy aims to bring you all the necessary transparency for a positive and confident experience with our services. Additional information may be provided to you as necessary when you sign up for a particular product or service.

Our privacy policy complies with global research industry Codes and Standards, as well as all pertinent laws governing privacy.

1.2.1 What Information Do We Collect

Information we collect falls into one of two categories: “voluntarily provided” information and “automatically collected” information.

“Voluntarily provided” information refers to any information you knowingly and actively provide us when using or participating in any of our services and promotions.

“Automatically collected” information refers to any information automatically sent by your devices while accessing our products and services.

We only collect and use your personal information lawfully, fairly, and in a transparent manner. We systematically respect the principle of minimization, which implies collecting and processing only what is strictly necessary to achieve our legitimate objective. We do not aim any of our products or services directly at children under the national child age consent, and we do not knowingly collect personal information about children under the national child age consent.

We process personal data that we need in order to carry out our business. We only process personal information in a way that is compatible with the purposes for which we collected it or subsequently authorized by the data subject. We take reasonable steps to ensure that personal data is reliable for its intended use, accurate, complete, and current.

The information notice that is sent to you before any collection or processing details the applicable legal basis, which depends on the services you use and how you use them. This means we only collect and use your information on the following grounds:

In order to respect your choice when we request consent from you:

“Personal information” only includes information relating to natural persons who can be identified or who are identifiable, directly from the information in question. Or who can be indirectly identified from that information in combination with other information. For example, name, contact details, location, consumer options/preferences, video/audio recordings... We may ask your consent for processing such information – for example, when you register an account or when you contact us via email, social media, or any similar technologies – which may include your name, your email, your phone/mobile number... When you contact us, you shall consent to your name and email address being used so we can respond to your inquiry.

Participation in all market research projects is voluntary and based on consent. Respondents may opt out of any market research project, at any time.

Personal information may also include **“Sensitive information”** or **“Special categories of data”** which is a subset of personal information that is given a higher level of protection. The types of sensitive information that we may collect about you include:

- Racial or ethnic origin
- Political opinions
- Religious or Philosophical beliefs
- Sexual orientation
- Sexual practices or sex life
- Medical or Health conditions
- Trade union membership

We will obtain your affirmative express consent (opt-in) if such information is to be (i) disclosed to a third party or (ii) used for a purpose other than those for which it was originally collected or subsequently authorized by the individuals through the exercise of your opt-in choice. We will also treat as sensitive any

personal information received from a third party where the third party identifies and treats it as sensitive.

In addition, we ensure that strengthened security measures are applied to these data, in order to avoid any breach of confidentiality, integrity, and availability.

A “**Cookie**” is a small piece of data that our website stores on your computer and accesses each time you visit. We use cookies to collect information about you and your activity across our site to understand how you use our site and to enable you to access and use our website. At all times, you may decline cookies from our site.

Please refer to our [Cookie Policy](#) for more information.

You may withdraw your consent at any time using the facilities we provide; however, this will not affect any use of your information that has already taken place.

While you may request that we delete your contact details at any time, we cannot recall any email we have already sent. If you have any further inquiries about how to withdraw your consent, please feel free to enquire using the details provided in the Contact Us section of this privacy policy.

In order to allow the performance of a contract or transaction at your request:

For example, if you purchase a product, service, or subscription from us, we may need to use your personal and payment information in order to process and deliver your order.

In order to follow our legitimate interests:

Where we assess whether it is necessary for our legitimate interests, such as for us to provide, operate, improve, and communicate our services, we consider our legitimate interests to include:

- research and development, understanding our audience, marketing and promoting our services, measures taken to operate our services efficiently, marketing analysis, and measures taken to protect our legal rights and interests,
- business development, including operating and improving our website, associated applications, and associated social media platforms,
- security and fraud prevention, and to ensure that our sites and apps are safe, secure, and used in line with our terms of use.

When you visit our website, our servers may automatically log the standard data provided by your web browser. It may include your device's Internet Protocol (IP) address, your browser type and version, the pages you visit, the time and date of your visit, the time spent on each page, and other details about your visit. The data we collect can depend on the individual settings of your device and software. We recommend checking the policies of your device manufacturer or software provider to learn what information they make available to us.

Additionally, if you encounter certain errors while using the site, we may automatically collect data about the error and the circumstances surrounding its occurrence. This data may include technical details about your device, what you were trying to do when the error happened, and other technical information relating to the problem. You may or may not receive notice of such errors, even at the moment they occur, that they have occurred, or what the nature of the error is.

Please be aware that while this information may not be personally identifying by itself, it may be possible to combine it with other data to personally identify individual persons.

“Transaction data” refers to data that accumulates over the normal course of operation on our platform. This may include transaction records, stored files, user profiles, analytics data, and other metrics, as well as other types of information, created or generated, as users interact with our services.

We consider **“User-generated content”** to be materials (text, image and/or video content) voluntarily supplied to us by our users for the purpose of publication, processing, or usage on our platform. All user-generated content is associated with the account or email address used to submit the materials.

Please be aware that any content you submit for the purpose of publication will be property of the client after posting (and subsequent review or vetting process). User-generated content cannot be used for purposes beyond market research (i.e., advertisements and customer testimonials) without express written permission. Once published, it may be accessible to third parties not covered under this privacy policy.

In order to comply with the law:

In some cases, we may have a legal obligation to use or keep your personal information. Such cases may include (but are not limited to) court orders, criminal investigations, government requests, and regulatory obligations. If you have any further inquiries about how we retain personal information in order to comply with the law, please feel free to enquire using the details provided in the Contact Us section of this privacy policy.

1.2.2 How Do We Ensure the Security of Your Personal Information

Because we are ISO 27001 certified, we comply with high international standards for computer security and the protection of personal information.

When we collect and process personal information, and while we retain this information, we will protect it within commercially acceptable means to prevent loss and theft, as well as unauthorized access, disclosure, copying, use, or modification.

You are responsible for selecting any password and its overall security strength, ensuring the security of your own information within the bounds of our services. For example, ensuring any passwords associated with accessing your personal information and accounts are secure and confidential.

We comply with laws applicable to us in respect of any data breach.

1.2.3 How Long Do We Keep Your Personal Information

We keep your personal information only for as long as we need to. This time period may depend on what we are using your information for, in accordance with this privacy policy.

For example, if you have provided us with personal information as part of creating an account with us, we may retain this information for the duration your account exists on our system. If your personal information is no longer required for this purpose, we will delete it or make it anonymous by removing all details that identify you.

However, if necessary, we may retain your personal information for our compliance with a legal, accounting, or reporting obligation (i) such as reporting of Incentive payments on a yearly basis to federal and/or state regulatory authorities pursuant to legal requirements or (ii) for archiving purposes in the

public interest, scientific, or historical research purposes or statistical purposes.

Except as otherwise permitted by law, regulation, or EU-U.S. Data Privacy Framework Principles, we destroy or anonymize personal data after it no longer serves a purpose of processing as contemplated above and/or once a lawful basis for processing it ceases to exist.

1.2.4 Who Are the Recipients of Your Personal Information and Where Are They Located

We may disclose personal information to:

- a parent, subsidiary, or affiliate of our company in order to provide product support
- third-party service providers for the purpose of enabling them to provide their services, including (without limitation) IT service providers, data storage, hosting and server providers, analytics, error loggers, debt collectors, maintenance or problem-solving providers, professional advisors, and payment systems operators
- our employees, contractors, and/or related entities in order to support the product
- our existing or potential agents or business partners in order to support the product
- credit reporting agencies, courts, tribunals, and regulatory authorities, in the event you fail to pay for goods or services we have provided to you
- courts, tribunals, regulatory authorities, and law enforcement officers, as required by law, in connection with any actual or prospective legal proceedings, or in order to establish, exercise, or defend our legal rights
- third parties, including agents or sub-contractors, who assist us in providing information, products, services, or direct marketing to you
- an entity that buys, or to which we transfer all or substantially all of our assets and business

Third parties we currently use include:

- Google Analytics for product usage metrics (unless prohibited by national data protection authorities)
- Google Ads and LinkedIn Insights Tag to measure our marketing campaigns
- Google Cloud Natural Language for text sentiment and for image analytics (brand/logo recognition)
- Azure Application Insights for logging and troubleshooting user issues
- Azure Cognitive Services for image analytics and machine text translation
- Amazon web services for data storage, compute, and image processing
- Help Scout for managing and responding to customer support requests
- Twilio for video interview capabilities
- Rev for video transcription services
- Hotjar for product usage metrics
- Drift Chatbot to help site visitors to navigate and make decisions
- Marketo (our Automation tool) to record and process user-submitted information
- Sense to get account insights
- Research Defender, Imperium, IPQualityScore, RelevantID, and MaxMind to identify suspicious respondents, eliminate fraudsters and bad actors, and ensure accurate and high-value datasets

If we or our assets are acquired, or in the unlikely event that we go out of business or enter bankruptcy, we would include data, including your personal information, among the assets transferred to any parties who acquire us. You acknowledge that such transfers may occur and that any parties who acquire us may, to the extent permitted by applicable law, continue to use your personal

information according to this policy, which they will be required to assume as it is the basis for any ownership or use rights we have over such information.

The personal information we collect is stored and/or processed in the United States, or where we or our partners, affiliates, and third-party providers maintain facilities.

The countries to which we store, process, or transfer your personal information may not have the same data protection laws as the country in which you initially provided the information. If we transfer your personal information to third parties in other countries: (i) we will perform those transfers in accordance with the requirements of applicable law; and (ii) we will protect the transferred personal information in accordance with this privacy policy.

1.2.5 Which Are the Security Measures in Place?

Access to private, sensitive, and confidential information, including your personal information, is restricted to authorized employees with legitimate business reasons.

All employees are expected to always maintain the confidentiality of personal information, and failure to do so will result in appropriate disciplinary measures.

We follow reasonable technical and management practices to help protect the confidentiality, security, and integrity of data stored on our system. While no computer system is completely secure, the measures implemented by our website reduce the likelihood of security problems to a level appropriate to the type of data involved. We employ physical, electronic, and procedural safeguards in connection with the collection, storage, and disclosure of any personal contact information. We encrypt the transmission of sensitive information using secure socket layer technology (SSL).

1.2.6 What Are Your Rights

- **Access:** You may request details of the personal information that we hold about you. We reserve the right to limit such access where the burden or expense of providing access would be disproportionate to the risks to your privacy in the case in question, or where the rights of persons other than you would be violated.
- **Your choice:** By providing personal information to us, you understand we will collect, hold, use, and disclose your personal information in accordance with this privacy policy. You do not have to provide personal information to us, however, if you do not, it may affect your use of our website or the products and/or services offered on or through it.
- **Information from third parties:** If we receive personal information about you from a third party, we will protect it as set out in this privacy policy. If you are a third party providing personal information about somebody else, you represent and warrant that you have such a person's consent to provide the personal information to us.
- **Marketing permission:** If you have previously agreed to us using your personal information for direct marketing purposes, you may change your mind at any time by contacting us using the details below.
- **Correction:** If you believe that any information, we hold about you is inaccurate, out of date, incomplete, irrelevant, or misleading, please contact us using the details provided in this privacy policy. We will take reasonable steps to correct any information found to be inaccurate, incomplete, misleading, or out of date.
- **Non-discrimination:** We will not discriminate against you for exercising any of your rights over your personal information. Unless your personal information is required to provide you with a particular service or offer (for example processing transaction data), we will not deny you goods or services and/or charge you different prices or rates for goods or services, including through granting discounts or other benefits, or imposing penalties, or provide you with a different level or quality of goods or services. Respondents are not discriminated against for their answers. Selection for participating in a study relies on research project objectives. Participation in studies is not related to any fees, and membership in our panel will also have no costs.

- **Complaints:** If you believe that we have breached a relevant data protection law and wish to make a complaint, please contact us using the details below and provide us with full details of the alleged breach. We will promptly investigate your complaint and respond to you, in writing, setting out the outcome of our investigation and the steps we will take to deal with your complaint. You also have the right to contact a regulatory body or data protection authority in relation to your complaint.

You have the right to choose (opt-out) whether your personal data is (i) to be disclosed to a third party or (ii) to be used for a purpose that is materially different from the purpose(s) for which it was originally collected or subsequently authorized by you. If you wish to opt out, all you need to do is contact us at compliance@sago.com. If you contact us to opt out, we will explain the options available and comply with your request as required by the Principles and the applicable law. Please note that applicable laws allow certain exceptions to your ability to opt-out, such as where we are parties to a contract that is still being performed, where the law requires us to maintain information for claims or tax reports, or otherwise. In such cases, we will retain and continue to use your information only to the extent permitted or required by law. The above opt-out right doesn't apply where the sharing of your personal data is with a third party who is acting as our agent (such as our service providers who perform services that help us to run our business). We won't provide your personal data to a third party under these circumstances unless we have a contract in place with that third party that requires the third party to comply with the DPF Principles.

Under European, Australian, and Canadian data protection laws, you also have the following rights:

- **Downloading of Personal Information:** We provide a means for you to be provided with the personal information you have shared through our site. Please contact us for more information.
- **Restrict:** You have the right to request that we restrict the processing of your personal information if (i) you are concerned about the accuracy of

your personal information; (ii) you believe your personal information has been unlawfully processed; (iii) you need us to maintain the personal information solely for the purpose of a legal claim; or (iv) we are in the process of considering your objection in relation to processing on the basis of legitimate interests.

- **Objecting to processing:** You have the right to object to the processing of your personal information that is based on our legitimate interests or public interest. If this is done, we must provide compelling legitimate grounds for the processing which overrides your interests, rights, and freedoms, in order to proceed with the processing of your personal information.
- **Data portability:** You may have the right to request a copy of the personal information we hold about you. Where possible, we will provide this information in CSV format or another easily readable machine format. You may also have the right to request that we transfer this personal information to a third party.
- **Deletion:** The data controller of a project may have a right to request that we delete the personal information we hold at any time, and we will take reasonable steps to delete personal information from our current records. If you ask us to delete your personal information, we will let you know how the deletion affects your use of our website or products and services. There may be exceptions to this right for specific legal reasons which, if applicable, we will set out for you in response to your request. If you terminate or delete your account, we will delete your personal information without undue delay. Please be aware that search engines and similar third parties may still retain copies of your personal information that has been made public at least once, like certain profile information and public comments, even after you have deleted the information from our services or deactivated your account.

We would respond to your requests without undue delay and at the latest within one month of receipt of your request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests.

1.3. United States Considerations

The purpose of this privacy policy is to inform you about the processing of your personal data by Sago and its entities in accordance with research industry Codes and Standards relating to the USA and additionally the country in which each Sago company is based.

Sago companies comply with all pertinent Federal and State laws governing privacy, including but not limited to the enacted California Consumer Privacy Act (CCPA) and recently amended California Privacy Rights Act (CPRA).

For questions or concerns relating to privacy, you may contact us by email at help@focusgroup.com.

All requests to exercise your rights must be accompanied by the details necessary to process your request. A copy of proof of identity may be requested if necessary.

1.4. European Considerations

The purpose of this privacy policy is to inform you about the processing of your personal data by Sago and its entities in accordance with the European Data Protection Regulation (the GDPR) and the UK GDPR, the amended French Data Protection Act, the new Spanish Fundamental Law on Data Protection (the NLOPD), the new German Federal Data Protection Act (the BDSG), and the UK Data Protection Act (the DPA).

Sago has signed internal EU Commission Standard Contractual Clauses and UK Addendum to safeguard its international transfers of personal data.

You have the right to lodge a complaint with [your national data protection authority](#). You can find more information about your data protection rights on your authority's website.

Sago has appointed a Data Privacy Officer in each European country to be your privileged interlocutor regarding the processing of your personal data. If you wish to contact a DPO, you can write to them at the following addresses:

- DE: de@sago.com
- FR: fr@sago.com
- SP: es@sago.com
- UK: uk@sago.com

All requests to exercise your rights must be accompanied by the details necessary to process your request. A copy of proof of identity may be requested if necessary.

1.5. Canadian Considerations

The purpose of this privacy policy is to inform you about the processing of your personal data by the Sago and its entities in accordance with the laws of Ontario and the applicable federal laws of Canada.

If you have any questions or comments about this Privacy Policy, you may contact us at methodify.support@sago.com or via postal mail at:

370 King St. West, 5th Floor, Box 4
Toronto, ON, Canada, M5V1J9

1.6. Australian Considerations

The purpose of this privacy policy is to inform you about the processing of your personal data by Sago and its entities in accordance with the federal Privacy Act, the Australian Privacy Principles, and States and Territories' legislations.

The Central Server is located in an Australian data centre with a fully redundant network with No Single Point of Failure, contains Multiple Layers of Network Security and is also secured with Windows Firewall and IPsec Policy.

You can change your information at any time, through the profile tab in your member portal. We are obliged by law to ensure that your information is accurate and up to date at all times.

If you have any queries or complaints in relation to your personal information, please don't hesitate to get in touch: help@focusgroup.com

You will need to outline what information you would like access to or identify your concerns. We will endeavour to respond to you within 3 business days.

1.7. Data Privacy Framework (DPF) Specificities

We comply with the EU-U.S. Data Privacy Framework (EU-U.S. DPF) and the UK Extension to the EU-U.S. DPF as set forth by the U.S. Department of Commerce. We have certified to the U.S. Department of Commerce that we adhere to the EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) with regard to the processing of personal data received from the European Union in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF. If there is any conflict between the terms in this privacy policy and the EU-U.S. DPF Principles, the Principles shall govern. To learn more about the DPF Program, and to view our certification, please visit <https://www.dataprivacyframework.gov/>. We commit to subject to the DPF Principles all the personal data received from the EU in reliance on the EU-U.S. for as long as we retain the personal data.

Sago receives personal data from EU and UK employees, respondents, panel members, clients, and website visitors. Sago will process their personal data for the following purposes:

Categories of Data Subjects	Purposes of the Processing of their Data	Categories of Third Parties Involved
EU and UK employees	<ul style="list-style-type: none"> · Support requests management · HR management · Data storage · Vouchers management 	<ul style="list-style-type: none"> · Bug tracking, incident management and project management system · Human resources management services · Data host
EU and UK respondents	<ul style="list-style-type: none"> · Project management · Requests management 	<ul style="list-style-type: none"> · Market Research services providers · Ticketing services
EU and UK panel members	<ul style="list-style-type: none"> · Panel Management · Requests management · Data storage 	<ul style="list-style-type: none"> · Data host · Ticketing services
EU and UK clients	<ul style="list-style-type: none"> · Relationship management · Business development 	<ul style="list-style-type: none"> · Customer relationship management solutions.
EU and UK websites' visitors	<ul style="list-style-type: none"> · To enable websites core features (like user logins) · To configure settings on the website visited (like language) · To provide with customized, enhanced, or optimized content and services · To measure the website performance and marketing campaign success 	<ul style="list-style-type: none"> · Cookies management platform

For complaints concerning Human Resources (HR) Personal Data and Personal Data other than HR, at no cost, you may file a complaint concerning how we process your Personal Data. We will take steps to remedy issues arising out of our alleged failure to comply with the DPF Principles. All you need to do is contact us at compliance@sago.com. If your complaint cannot be resolved through our internal processes, we cooperate with the panel established by the Data Protection Authorities (DPAs).

Under certain circumstances and following the procedures and subject to conditions set forth in the DPF Annex I, you may also be able to invoke binding arbitration to address complaints about Sago's compliance with the DPF Principles.

We are subject to the investigatory and enforcement powers of the FTC, the DOT or any other U.S. authorized statutory body.

We will disclose personal data in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

When we transfer personal data to a third party acting as a controller, we comply with the DPF Principles. We also enter into a contract with the third-party controller that provides that such data may only be processed for limited and specified purposes consistent with your consent and that the recipient will provide the same level of protection as the DPF Principles and will notify us if it makes a determination that it can no longer meet this obligation. Those contracts provide that, when such a determination is made, the third-party controller ceases processing or takes other reasonable and appropriate steps to remediate.

When we transfer personal data to a third party acting as an agent, (i) we transfer such data only for limited and specified purposes; (ii) we require (usually

by contract) at least the same level of privacy protection as is required by the DPF Principles; (iii) we take reasonable and appropriate steps to ensure that the agent effectively processes the personal data transferred in a manner consistent with the organization's obligations under the Principles; (iv) we require the agent to notify us if it makes a determination that it can no longer meet its obligation to provide the same level of protection as is required by the Principles; (v) upon notice, including under (iv), we take reasonable and appropriate steps to stop and remediate unauthorized processing; and (vi) we will provide a summary or a representative copy of the relevant privacy provisions of our contract with that agent to the Department of Commerce upon request.

If we transfer personal data to a third party acting as an agent on our behalf who processes such data in a manner inconsistent with the DPF Principles, we remain liable under the DPF Principles, unless we prove that we are not responsible for the event giving rise to the damage.

In compliance with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF, we commit to cooperate and comply respectively with the advice of the panel established by the EU data protection authorities (DPAs) and the UK Information Commissioner's Office (ICO) with regard to unresolved complaints concerning our handling of personal data received in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF.

When we become subject to a court order that is based on non-compliance or an order from a U.S. statutory body (e.g., FTC or DOT) listed in the DPF Principles or in a future annex to the Principles that is based on non-compliance, we will make public any relevant EU-U.S. DPF-related sections of any compliance or assessment report submitted to the court or U.S. statutory body to the extent consistent with confidentiality requirements.

1.8. How Can You Find Out About Changes to This Policy

At our discretion, we may change our privacy policy to reflect updates to our business processes, current acceptable practices, or legislative or regulatory changes. If we decide to change this privacy policy, we will post the changes here at the same link by which you are accessing this privacy policy.

If the changes are significant, or if required by applicable law, we will contact you (based on your selected preferences for communications from us) and all our registered users with the new details and links to the updated or changed policy.

If required by law, we will get your permission or give you the opportunity to opt in to or opt out of, as applicable, any new uses of your personal information.

1.9. Contact Us

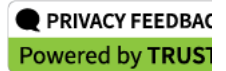
For any general questions or concerns regarding your privacy, you may contact us using the following details:

US	<ul style="list-style-type: none">• help@focusgroup.com
EU	<ul style="list-style-type: none">• DE: dpo.de@sago.com• FR: dpo.fr@sago.com• SP: dpo.es@sago.com• UK: dpo.uk@sago.com
Canada	<ul style="list-style-type: none">• methodify.support@sago.com
Australia	<ul style="list-style-type: none">• help@focusgroup.com



Toluna Influencers Panel Privacy Notice

Last updated: January 2022



Who are we?

We are Toluna Group Limited, part of the Toluna Holdings Limited worldwide group ("**We**" "**Our**" "**Us**" or "**Toluna**"). You can see who our group members are by clicking on the link below:

<https://tolunacorporate.com/locations/>

Toluna are an online data collection group focused on providing high-quality market research data to its clients who are in various business sectors, including other market research agencies and other global and corporate clients of all sizes. We also build and maintain large online consumer panels, providing real-time digital consumer insights to our clients via our market research surveys and analytics platforms.

The Toluna company with whom you registered as a Member is the controller and responsible for your personal data.

We have appointed a data protection officer (DPO) who is responsible for overseeing questions in relation to this privacy notice. If you have any questions about this privacy notice, including any requests to exercise your legal rights, please contact the DPO at [\[Contact Us\]](#).

This privacy notice does not apply where you have agreed to participate in surveys administered by third parties. In these situations, Toluna is not the sponsor of the survey and the technologies/media of those surveys and the survey results or survey data are and will be controlled by the sponsor of those surveys. Please refer to the relevant sponsor's privacy policy to learn more about those sponsor's privacy practices.

What is our Privacy Commitment to you?

We respect your privacy and are committed to protecting your personal data. This privacy notice describes how we collect, use, share and secure personal data you provide on <http://www.influencers.toluna.com> (our "**site**") and/or via our Mobile app when you become a member of our influencers panel and participate in surveys and/or research studies ("**surveys**") that we conduct for, and on behalf of our clients. It also explains your privacy rights and how laws that are applicable to you may protect you and is intended to supplement other notices and privacy policies and not to override them.

The registration, use of and access to your Membership and use of our systems and media ("**Services**") is subject to this privacy notice.

This privacy notice is provided in a layered format so you can click through to the specific areas set out below. Please also use the Glossary to understand the meaning of some of the terms used in this privacy notice.



Frequently asked questions:

- [Who are we?](#)
- [What is our Privacy Commitment to you?](#)
- [What personal data do we collect about you?](#)
- [How do we use your personal data?](#)
- [Who do we share your personal data with?](#)
- [Do we transfer your personal data to other countries?](#)
- [What other ways can you become a member of our influencers panel? – Our mobile app](#)
- [What cookies do we use on our site?](#)
- [What other tracking technologies do we use for surveys you participate in and for other purposes?](#)
- [What is our winner's policy and privacy guarantee?](#)
- [What security measures do we undertake to protect your personal data?](#)
- [What are our data retention and destruction policies?](#)
- [Business Transfers](#)
- [Links](#)
- [Children's privacy](#)
- [Your rights](#)
 - [How do you access your information; use the member services area and/or update, correct or delete your information?](#)
 - [How do you terminate your influencers' panel membership?](#)
 - [Data Retention](#)
 - [How do you ask a question or make a complaint?](#)
 - [Your other rights](#)
 - [Your rights in California](#)
- [Changes to the privacy notice and your duty to inform us of changes](#)
- [Privacy contact details](#)

What personal data do we collect about you?

Personal data means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (i.e. anonymous data).

We may collect, use, store and transfer different kinds of personal data about you which we have grouped together follows:

- **(A) Identity data** – name (includes first, last, maiden and married names), date of birth, marital status, gender, panelist id, and username.
- **(B) Contact data** – postal address, email address, and telephone number.

- **(C) Special categories of personal data** – ethnic/racial origin, health, genetics, political opinion, religion, sexual orientation and sex life.
- **(D) Demographic/Profile data** – interests, preferences, feedback and survey responses and including, but not limited to; age, marital status, gender, birthday, household size, income, education, and employment status.
- **(E) Technical data** includes internet protocol (IP) addresses, login data, browser type, and version, time zone setting and location, browser plug-in types and versions, operating system and platform and other technology on the devices you use to access this website.
- **(F) Pseudonymized data** are identifiable data as unique identifiers e.g. panelist ID's or Technical data are used, however direct identifiers, such as; name and Contact data are removed.

Influencers Panel Members

When you agree to become a member of our influencers panel ("**Member**"), you are able to participate in our surveys. We will ask you to complete the registration form via <https://influencers.toluna.com> (our "**site**") or via links displayed on our partners' websites and you may also register to be a Member via our mobile app.

Non-members of our Influencers Panel

If you are not a Member of our influencers panel ("**non-member**"), but take a survey with us and provide us with your personal data, the only personal data we may preserve about you is your email address, gender, age information, full or partial zip/postal code, machine ID and IP address. We do this so we may:

- contact you if you have won a prize or are entitled to an incentive, in which case, we will collect and maintain such personal data, to the extent required by any applicable law or regulation (e.g. for tax reasons, if applicable);
- to match you against the survey you are taking; and
- improve the user experience.

We will not contact you for any other reason.

Public forums and blogs

Our website offers publicly accessible blogs or community forums. You should be aware that any information you provide in the areas may be read, collected, and used by others who access them.

We display personal testimonials of satisfied customers on our site in addition to other endorsements. With your consent, we may post your testimonial along with your username. If you wish to update or delete your testimonial, you can contact us at [\[Contact Us\]](#).

You should be aware that any personal data you choose to make public on the site, in the Community area (under a public message on your wall, as an opinion, topic, battle, thumb it, or any other public area or forum) can be read, collected, stored and/or used by other users and could be used to send you unsolicited messages.

We strongly discourage you from disclosing any of your personal data in any public forum or community area that you may find on the site and in particular, we would never ask you to provide your Contact data or Identity data on a public community area, even if it was part of a survey. We cannot guarantee that third parties with whom you share your personal data via those public forums or community areas will keep them secure or confidential. Please be aware that we are not responsible for the personal data you choose to submit or make public. In addition, we are not responsible for the content you publicly post on the site that can be found via web-based search engines.

How do we use your personal data?

In the table below, we have set out a more detailed explanation of the ways in which we use your personal data. Where we use any third parties for modelling, analytical or data matching purposes, please be assured that such parties are not allowed to use your personal data for any reason, other than the reasons we state in the table and we enter into contracts with those third

parties to ensure your data is kept secure, confidential and erased in accordance with our data retention and destruction policies as set out in our Panelist Privacy Notice.

In many countries, we are required by law to explain the legal bases we rely on when we process your personal data. These legal bases are listed as follows and we may use more than one lawful basis when processing your personal data.

Consent – In certain cases, we collect and process your personal data with your consent e.g. when you participate in surveys, we will ask you if you wish to participate.

Contractual obligations – In some circumstances, we need to process your personal data to comply with a contractual obligation e.g. when we use your personal data to send you your rewards.

Legal compliance – If the law requires us to, we may need to collect and process your personal data in response to lawful requests by public authorities or if e.g. we believe in good faith that disclosure is necessary to protect our rights, to protect your safety or the safety of others, to investigate fraud or breaches of our site terms, or to respond to a government request.

Legitimate interest – means the interest of our business in conducting and managing our business to enable us to give you the best service/product and the best and most secure experience. We make sure we consider and balance any potential impact on you (both positive and negative) and your rights before we process your personal data for our legitimate interests. We do not use your personal data for activities where our interests are overridden by the impact on you (unless we have your consent or are otherwise required or permitted to by law).

Your Membership (2)
Market research surveys
Scientific research/Safety monitoring (Pharmacovigilance Adverse Events Reporting)
Mobile Device surveys and usage
Profiling
Data matching and enrichment
Ad-Effectiveness campaigns & look-a-likes
Ad exposure and measurement
Legal/public authority disclosure
Fraudulent and quality checking

Who do we share your personal data with?

Any of our group members found at <https://tolunacorporate.com/locations> may access or use your personal data for the purposes set out in table above and/or to carry out our regular business activities, such as to provide, maintain and personalize our sites and services, to communicate with you, and to accomplish our legitimate business purposes, pursuant to contractual safeguards.

In general, responses we collect from you via our surveys are provided to our clients either in anonymized and aggregated form or in pseudonymized form. If we provide the results in anonymized and aggregated form, the results include information about groups of individuals and not on an individual level. If we provide the results in pseudonymized form, the results will be on an individual basis, using unique identifiers, such as your assigned panelist ID, but will not include your Identity data or Contact data.

Identity data or Contact data about you would only be provided to our clients in specific surveys for the purposes of research and we would never provide such data to our clients unless we have first received your consent and confirmed with them that their use is in accordance with applicable law and market research codes of practice.

From time to time we may engage third parties to issue you with cheques or processing the delivery of your rewards and /or other third parties for the purposes of those parties providing us or our clients with services such as; data processing or analytic services or to append data they previously collected about you. Such third parties are not allowed to use your personal data for any other reason and we enter into contracts with those third parties to ensure your personal data is kept secure and erased in accordance with our data retention and destruction policies.

From time to time, Toluna may use third-party software for email list management and email distribution or may use third-party list management providers to match our Members to members of other lists or panels or to validate the accuracy of personal data you provide. These companies are authorized to use your personal data only as necessary to provide these services to us, pursuant to written instructions. In such cases, these companies must abide by our data privacy and security requirements and are not allowed to use personal data they receive from us for any other purpose.

Though we make every effort to preserve your privacy, we may be required to disclose your personal data in response to lawful requests by public authorities, including to meet national security or law enforcement requirements. We may also disclose your personal information as required by law, such as to comply with a subpoena or other legal process, when we believe in good faith

that disclosure is necessary to protect our rights, to protect your safety or the safety of others, to investigate fraud or breaches of our site terms, or to respond to a government request.

Please see the [table above](#) for more on these uses.

Do we transfer your personal data to other countries?

Toluna is a global company and your personal data is transferred to other members of the Toluna group of companies and our trusted service providers, who are located in countries other than where you live. Please be aware that laws in other countries may differ from the laws applicable in your own country of residence. See in the attached list of all the Toluna companies: <https://tolunacorporate.com/about>.

Toluna USA Inc., - The EU-U.S. Privacy Shield Framework

Our global back up and hosting service centre is located in the USA. Toluna USA Inc., ("**Toluna USA**") is a member of the Toluna group of companies and all data we use are transferred to Toluna USA for those purposes. Toluna USA recognises that the EEA have established strict protections regarding the handling of personal data from the EEA, including requirements to provide adequate protection for such personal data transferred outside of the EEA. Toluna ensures that it provides adequate protection for the processing of certain EEA personal data about all individuals (including about you).

Toluna USA participates in and has certified its compliance with the EU-US Privacy Shield Framework. Toluna is committed to subjecting all personal data received from European Union (EU) member countries, in reliance on the Privacy Shield Framework to the Framework's applicable Principles. To learn more about the Privacy Shield Framework, visit the U.S. Department of Commerce's Privacy Shield List. [<https://www.privacyshield.gov/list>].

Toluna USA is responsible for the processing of personal data it receives, under the Privacy Shield Framework, and subsequently transfers to a third party acting as an agent on its behalf (Iron Mountain). Toluna USA complies with the Privacy Shield Principles for all onward transfers of personal data from the EU and Switzerland, including the onward transfer liability provisions. If there is any conflict between the terms of this privacy notice and the Privacy Shield Principles, the Privacy Shield Principles shall govern.

With respect to personal data received or transferred pursuant to the Privacy Shield Framework, Toluna is subject to the regulatory enforcement powers of the US Federal Trade Commission. For more information about the Privacy Shield, see the U.S. Department of Commerce's Privacy Shield website located at <https://www.privacyshield.gov>. In certain circumstances, we may be required to disclose personal data in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

In compliance with the Privacy Shield Principles, Toluna USA commits to resolve complaints about its collection or use of your personal data. EEA individuals with enquiries or complaints regarding our Privacy Shield policy should first contact the Data Protection Officer at [[Contact Us](#)].

If you have an unresolved privacy or data use concern that we have not addressed satisfactorily, please contact our U.S.-based third party dispute resolution provider (free of charge) at feedback-form.truste.com/watchdog/request.

Under certain conditions, more fully described on the Privacy Shield website <https://www.privacyshield.gov/article?id=How-to-Submit-a-Complaint>, you may be entitled to invoke binding arbitration when other dispute resolution procedures have been exhausted.

You may have the option to select binding arbitration for the resolution of your complaint under certain circumstances, provided you have taken the following steps: (1) raised your complaint directly with Toluna and provided us the opportunity to resolve the issue; (2) made use of the independent dispute resolution mechanism identified under the How do you ask a question or make complaint? paragraph below; and (3) raised the issue through the relevant data protection authority and allowed the US Department of Commerce an opportunity to resolve the complaint at no cost to you. For more information on binding arbitration see the US Department of Commerce Privacy Shield Framework: Annex 1 (Binding Arbitration) at <https://www.privacyshield.gov/EU-US-Framework>.

What other ways can you become a member of our influencers panel? – Our mobile app

Mobile Applications

You may choose to become a Member by using our mobile application (app). When you download and use our mobile app, we automatically collect system and performance information on the type of device you use, operating system version, device identifier and hardware usage statistics such as CPU, RAM, storage, and app version. We will use the information we collect via our mobile app in accordance with the terms of this privacy notice and the provisions set out below.

We send you push notifications from time-to-time in order to notify you about surveys and ask you if you would like to participate in certain marketing research studies in accordance with this privacy notice. If you no longer wish to receive these types of communications, you may turn them off at the device level. To ensure you receive proper notifications, we will need to collect certain information about your device such as operating system and user identification information.

SMS

We may make available a service either directly or through third parties by which you can receive messages on your wireless device via short message service ("SMS Service")

Your provider's standard data and messaging rates apply to all SMS correspondence. All charges are billed by and payable to your mobile service provider. You represent that you are the owner or authorised user of the wireless device on which message will be received and that you are authorised to approve the applicable charges. Personal data obtained from you in connection with this SMS Service may include your Identity data and Contact data, your provider's name, and the date, time, and content of your messages. The use of this information will be in accordance with this privacy notice. If fees are charged to your wireless account invoice, we may be required to provide your carrier with your Identity data and Contact data in connection therewith. Your wireless carrier and other service providers may also collect data about your wireless device usage, and their practices are governed by their own policies. You acknowledge and agree that the SMS Service is provided via wireless systems which use radios (and other means) to transmit communications over complex networks. We will not be liable for any delays in the receipt of any SMS messages, as delivery is subject to effective transmission from your network operator. SMS message services are provided on an as-is basis. We do not guarantee that your use of the SMS Service will be private or secure, and we are not liable to you for any lack of privacy or security you may experience. You are fully responsible for taking precautions and providing security measures best suited for your situation and intended use of the SMS Service. You can opt out from this service at any time by going to your [account page](#) and unticking the option "I agree to receive invitations to surveys by SMS" in the Personal Details tab. If available in your country, you may also be able to opt out by text by following the instructions given to you in the SMS we send you.

Single Sign-ON

You can log in to our site using sign-in services such as Facebook Connect or an Open ID provider. These services will authenticate your identity and provide you with the option of becoming a Member. Services like Facebook Connect give you the option to post information about your activities on this site to your profile page to share with others within your network.

Referral

If you choose to use our referral service to tell a friend about our site, you may pass your unique referral link to your friend and if your friend becomes a Member, we will provide you with Toluna points as a reward.

What cookies do we use on our site?

Our site uses cookies to distinguish you from other users of our site, and estimate visits and click throughs for specific campaigns. This helps us to provide you with a good experience when you browse our site and also allows us to improve our site. These cookies expire when your browsing session ends. By continuing to browse the site, you are agreeing to our use of cookies.

A cookie is a small file of letters and numbers that we store on your browser or the hard drive of your computer if you agree. Cookies contain information that is transferred to your computer's hard drive.

For detailed information on the cookies we use and the purposes for which we use them, see our cookie policy at: <https://www.influencers.toluna.com/cookie-policy>.

What other Tracking Technologies do we use for surveys you participate in and for other purposes?

Surveys - client cookie tracking, including for Ad effectiveness campaigns

We may share your unique panellist ID (UID) with our clients, who may write, set or read cookies or use other Technical data about you from multiple locations, including our own servers or systems. If you participate, your UID will be stored or associated with those Technical data to allow us and/or our clients to conduct online ad-effectiveness campaigns, track your visits to websites, use your Demographic/Profile data to create look-a-like segments and/or gain other online insights about you. If you have interacted with the online ad or promotion, our client will send your UID and the specific survey to us and we may provide you with the opportunity to complete the survey.

Other Technologies

Automated technologies or interactions.

As you interact with the site, we will automatically collect Technical data about your equipment, browsing actions and patterns. We collect this Technical data by using cookies, server logs, digital finger printing technologies and other similar technologies. We may also receive Technical data about you if you visit other websites employing our cookies. Please see our [cookie policy](#) for further details.

Server log files:

We may collect Internet protocol (IP) addresses, browser type, internet service provider (ISP), referring/exit pages, operating system, date/time stamp, and/or clickstream data. This Technical data may be combined with other information collected about you for the purposes of improving our services, site functionality and collecting analytical data.

Fingerprinting technologies:

In general, digital Fingerprinting technologies assign a unique identifier or "Machine-ID" to a user's computer to identify and track your device ("Technology"). The Technology will analyse publicly available information and data obtained from your computer's web browser and from other publicly available data points, including the technical settings of your computer, the characteristics of your computer, and its IP Address, to create a unique identifier, which will be assigned to your device. We use the Technology for quality control, validation, and fraud detection and prevention purposes, including assisting us in ensuring the integrity of survey results. Appropriate technical and operational processes and procedures will be put in place to ensure that the Technology is safe, secure and does not cause undue privacy or data security risks and the Technology will be used and distributed in a professional and ethical manner and in accordance with (a) this privacy notice, (b) any other statements and/or disclosures made to you as a member of the community and (c) applicable laws and market research codes of practice. In the event any unethical conduct is discovered in connection with the use of the Technology, or that the Technology is being used in a manner that is

inconsistent with privacy notice, immediate action will be taken to prohibit such unethical conduct and to ensure the proper administration of the Technology.

Advertising

We partner with third parties to either display advertising on our site or to manage our advertising on other sites. Our third-party partners may use technologies such as cookies to gather information about your activities on their site and other sites in order to provide you advertising based upon your browsing activities and interests. If you wish to not have this information used for the purpose of serving you interest-based ads, you may opt-out by clicking [here](#). Please note this does not opt you out of being served ads. You will continue to receive generic ads.

Digital Fingerprinting

In general, digital Fingerprinting technologies assign a unique identifier or "Machine-ID" to a user's computer to identify and track your computer. We will not use digital fingerprinting technology (the "Technology") to collect your Identity or Contact data, or track your online activities; and will not disrupt or interfere with the use or control of your computer or alter, modify or change its settings or functionality. Occasionally, in specific market research programs, we will use the Technology to assist our clients in ensuring the integrity of survey results. The Technology will analyse publicly available information and data obtained from your computer's web browser and from other publicly available data points, including the technical settings of your computer, the characteristics of your computer, and its IP Address, to create a unique identifier, which will be assigned to your computer. The unique identifier will be an alpha-numeric ID. In order to assist our clients in protecting and ensuring the integrity of survey results we may; (a) link or associate your unique identifier to you and any of your personal data; (b) share your unique identifier with our clients and with other sample or panel providers; and (c) receive or obtain a unique identifier linked to you from a third party, including without limitation a sample or panel provider or our client, however we will only provide such information to any third parties (including our clients) on an aggregated and anonymised or pseudonymised basis. In addition, any unique identifier(s) received or obtained by us and linked to you will be protected in accordance with this privacy notice and if required by law, we will ask for your consent in advance.

We shall do everything we can to ensure that the Technology is safe, secure and does not cause undue privacy or data security risks and we shall use and distribute the Technology in a professional and ethical manner and in accordance with (a) this privacy notice, (b) any other statements and/or disclosures made by us to you and (c) applicable laws and market research codes of practice. In the event that we discover or learn of any unethical conduct in connection with the use of the Technology, or that the Technology is being used in a manner that is inconsistent with the statements and/or disclosures made by us to you or is in breach of applicable laws and the market research codes of conduct, we will take immediate action to prohibit such unethical conduct and to ensure the proper administration of the Technology.

Social Media Widgets

Our site includes Social Media Features, such as the Facebook Like button (and Widgets, such as the Share This Button or interactive mini-programs that run on our site). These Features may collect your IP address; which page you are visiting on our site; and may set a cookie to enable the Feature to function properly. Social Media Features and Widgets are either hosted by a third party or hosted directly on our site. Your interactions with these Features are governed by the privacy notice of the company providing it.

What is our winner's policy and privacy guarantee?

Members and others who take our surveys are randomly selected to win prizes for participation in surveys, content, games and other promotions. All winners are notified by email or via our site of their winnings. Toluna shall post the usernames of winners on our site and on our own blogs and newsletters. For more information, please visit our [Terms and Conditions](#) page. Cash and other prizes awarded to non-members will be awarded directly.

What security measures do we undertake to protect your personal data?

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or access in an unauthorised way, altered or disclosed. In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal data on our instructions, and they are subject to a duty of confidentiality.

Although we do everything we can to keep your data safe, unfortunately no systems can guarantee they are 100% secure. If you have questions about the security of your personal data, or if you have reason to believe that the personal data that we hold about you is no longer secure, please contact us immediately as described in this Privacy Notice.

We have put in place procedures to deal with any suspected personal data breach and will notify you and any applicable regulator or supervisory authority of a breach where we are legally required to do so.

What are our data retention and destruction policies?

How long will you use my personal data for?

We will only retain your personal data for as long as necessary to fulfil the purposes we collected it for, including for the purpose of satisfying any legal, accounting, or reporting requirements.

To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

As the results of the surveys and other aggregated or Pseudonymised data are used for research, scientific, historical and/or statistical purposes (whether publicly or privately funded), we and our clients or other third parties may use this information for such purposes in accordance with the terms indefinitely without further notice to you.

Business Transfers

As we continue to develop our business, we might sell or buy additional assets. In such transactions, Toluna's right to contact you as a Member and the information you have voluntarily provided in your user profile would generally be one of the transferred business assets. Any merger, sale or transfer of Toluna of substantially or all of its business assets (which included our influence panel), or other fundamental corporate transaction would be to an entity that agreed to comply with all of the material terms of our privacy notice. You will be notified via email and/or a prominent notice will be posted on our site if any transaction may result in any new proposed uses of your personal data which are incompatible with the uses set out in this Privacy Notice and of the choices you may have regarding your personal data.

Links

From time to time we may offer visitors the ability to voluntarily link to other sites. Toluna does not review, and is not responsible for, the content or effect of the privacy policies of these sites.

Children's privacy

Toluna will not knowingly collect any information from any child under the age of 16 without permission from his/her parents, legal guardian or an adult responsible for the care of the child. Eligible 'young people' (individuals aged between 16 and 17) may be invited to participate in our Teens panel from time to time. We comply with COPPA, the EU "Safer Internet programme", the General Data Protection Regulations and the ESOMAR guidelines in relation to surveys concerning children and young people. If you are a parent or guardian of a child under 16 and become aware that your child has provided personal data to us and you are not aware of such processing, please contact us as described in this Privacy Notice and we will take reasonable steps immediately to remove any such information.

Your rights

How do you access your information; use the member services area and/or update, correct or delete your information?

Upon request, Toluna will provide you with information about whether we hold any of your personal data. You may access, correct, or request deletion of your personal data, or terminate your membership by logging into your Member Account. By following the appropriate directions, your information should be automatically updated in our database. For these purposes, and if you are unable to correct your personal data yourself via the [Account](#), you may write to us at the postal address found at the end of this privacy notice, or contact us [here](#). We will respond to all requests within a reasonable timeframe.

How do you terminate your panel membership?

If you choose to end your membership with Toluna or to require us to cease processing your personal data, you may discontinue your membership by going to "Account" and selecting the "Unsubscribe" tab or by going directly to the page "[Unsubscribe page](#)". By following the appropriate directions, your record will be marked as "do not contact", and you will no longer receive communications from Toluna. In addition, you will forfeit any incentive balance that has not been requested as of the time you opt out. As an alternative, you may send an email directly using the [Contact us](#) form requesting to be removed. Email links are provided on the site so that you may contact us directly with any questions or concerns you may have. Each email we receive is read and responded to individually. In most cases it will take 2 to 3 days to process this change, but please allow up to two full weeks for your status to be finalised. Please note that you may continue to receive communications during this short period after changing your preferences while our systems are fully updated.

Data Retention

If you terminate your membership, we will no longer use your personal data to contact you, but in accordance with our backup procedures, we will retain your personal data until your personal data are eventually destroyed in accordance with our data retention and destruction policies and we will continue to employ the security procedures and technologies to keep your personal data safe.

How do you ask a question or make a complaint?

You can direct any questions or complaints about the use or disclosure of your personal data to our [Privacy Contact](#). We will investigate and attempt to resolve any complaints or disputes regarding the use or disclosure of your personal data within 30

days of receiving your complaint.

If you have an unresolved privacy or data use concern that we have not addressed satisfactorily, please contact our U.S.-based third-party dispute resolution provider (free of charge) at <https://feedback-form.truste.com/watchdog/request>. Under certain conditions, more fully described on the Privacy Shield website <https://www.privacyshield.gov/article?id=How-to-Submit-a-Complaint>, you may invoke binding arbitration when other dispute resolution procedures have been exhausted.

Your other rights

You may:

- **request access** to your personal data and we may conduct ID checks before we can respond to your request.
- **have your personal data erased, corrected or restricted** if it is inaccurate or requires updating. You may also have the right under certain circumstances to request deletion of your personal data; however, this is not always possible due to legal requirements and other obligations and factors. You can update your account information via your Account or by contacting us at the address given below.
- **object to the processing your personal data** if we are not using your personal data for the purposes set out in this privacy policy.

Your rights in California

You have certain rights under the California Consumer Privacy Act 2018 (CCPA) if you are citizen of California. You can exercise the above rights by:

- Calling us on our toll-free number [877-438-4224].
- Email us at [\[Contact US\]](#).
- Writing to us at the address given under the Privacy Contact Details; or
- Following the process under the paragraph **How do we terminate your influencer panel membership?** above

If you wish to opt out of our Membership program, you may do so in accordance with the process under the paragraph **How do we terminate your influencers panel membership?** above. Once you make an opt-out request, we will remove you from our Influencer panel and we will not contact you again unless you decide to re-register with us.

We will not discriminate against you for exercising any of your CCPA rights. Unless permitted by the CCPA, we will not exclude you from participating in any Surveys you may be eligible for on the basis of you exercising your CCPA rights.

Please note that you do not have the right to the erasure of the results of any surveys you participated in and we have provided to our clients in accordance with uses set out in the table under [\[How do we use your personal data?\]](#). Those results may include your Demographic and Profile data and/or Technical data but will not include any of your Identity data or Contact data allowing you to be directly identified. We don't erase the results of the Surveys you participated in because we provide you with certain financial incentives as permitted by the CCPA. When you became a Member, you opted in to participate in Surveys from time to time and by way of a contract between you and us, we have provided you with certain rewards, such as; Toluna points and/or participation in our sweepstakes in return for; your time; your participation in surveys; and giving us your opinions. The rules on those rewards are found here: <https://www.toluna.com/Terms>

Changes to the privacy notice and your duty to inform us of changes

This version was last updated on the date at the top of this privacy policy.

We reserve the right to modify this privacy statement at any time, so please review it frequently. If we do decide to change our privacy notice, we will post those changes to this privacy statement on the homepage, or other places we deem appropriate so that you are aware of what information we collect, how we use it, and under what circumstances, if any, we disclose it. If we

make material changes to this policy, we will notify you here, by email, or by means of a notice on our home page prior to the change becoming effective.

It is important that the personal data we hold about you is accurate and current. Please keep your Account details updated if your personal data changes during your relationship with us.

Privacy contact details

You may contact us by writing to:

The Data Protection Officer
Toluna
85 Uxbridge Road
W5 5TH
London

[Privacy Policy | Prodege : Prodege](#)

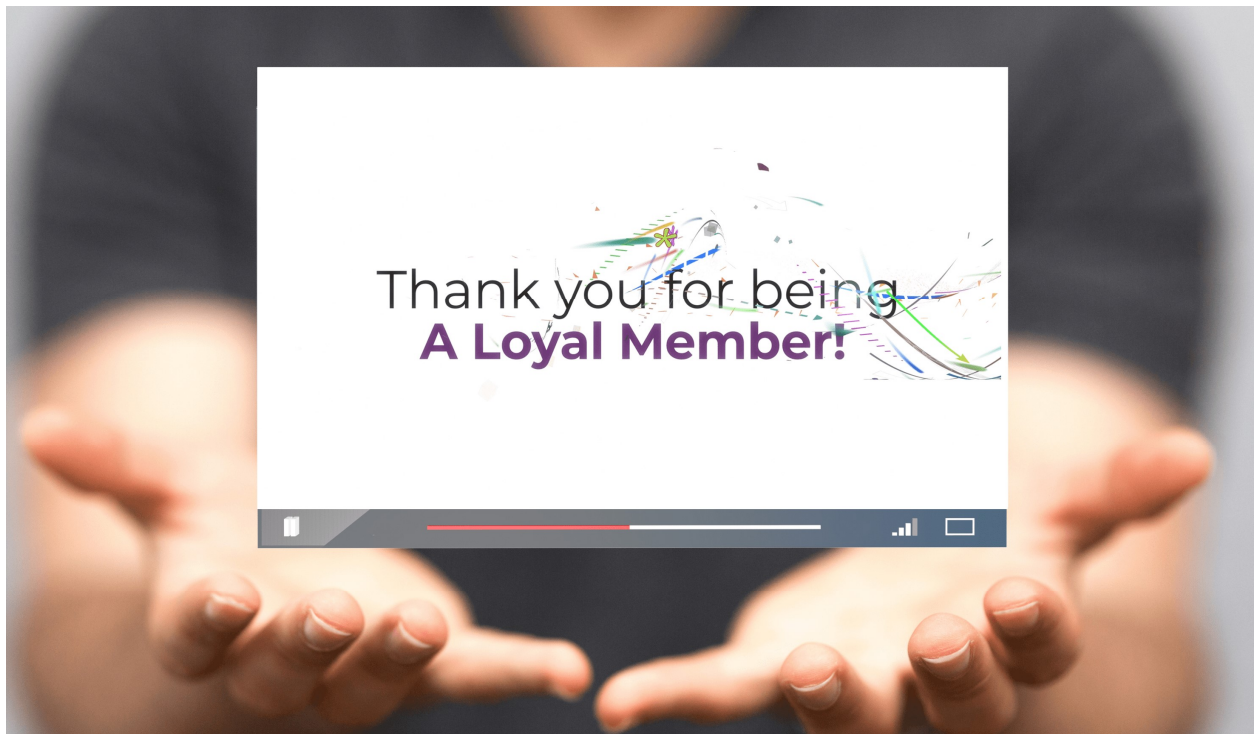
Please note: This website includes an accessibility system. Press Control-F11 to adjust the website to the visually impaired who are using a screen reader; Press Control-F10 to open an accessibility menu.

Accessibility

- Press enter for Accessibility for blind people who use screen readers
- Press enter for Keyboard Navigation
- Press enter for Accessibility menu

Privacy Policy

United States and Canada



-
- **NEW PRIVACY POLICY**
 - **1. Introduction**
 - **2. Information We Collect Directly**
 - **3. Information We Receive from Third Parties**
 - **4. Use and Sharing of Information**
 - **5. Friend Referrals**
 - **6. Community Features and User Content**
 - **7. Third Party Services**
 - **8. Advertising Networks**

- [**9. Session Replay and Analytics Companies**](#)
- [**10. Cookies and Tracking Technologies**](#)
- [**11. Card Linked Offers Programs**](#)
- [**12. Social Features**](#)
- [**13. Disclosure of Data**](#)
- [**14. Business Transactions**](#)
- [**15. Updating Your Information, Choice and Opt-Out**](#)
- [**16. Notification of Privacy Policy Updates**](#)
- [**17. Children's Privacy**](#)
- [**18. Security**](#)
- [**19. Location of Processing and Applicable Law**](#)
- [**20. Contact Us**](#)
- [**U.S. STATE PRIVACY NOTICE**](#)
- [**A. Notice of Data Practices**](#)
- [**B. Your Consumer Rights and How to Exercise Them**](#)
- [**C. How We Process Your Consumer Privacy Requests**](#)
- [**D. Non-Discrimination/Non-Retaliation**](#)
- [**E. Notice of Financial Incentive Programs**](#)
- [**F. Our Rights and the Rights of Others**](#)
- [**G. Additional Notices for California Residents**](#)

Looking for Customer Support?

Find the Help Centers Below:

SwagbucksInboxDollarsMyPointsUpromiseTadaySense

NEW PRIVACY POLICY

This Privacy Policy was last updated on: August 1, 2023

1. Introduction

This "Privacy Policy" is for residents and persons located within the United States and Canada. For all other visitors, please visit the international version of our Privacy Policy [here](#). We want you to be familiar with how we collect, use, and share your Personally Identifiable Information (defined below). This Privacy Policy outlines the type of information that we collect and receive from and about you via the Prodege Sites and Features and our Services (both as defined below), and our data practices related thereto, with additional disclosures for California, Colorado, Connecticut, Nevada, Utah and Virginia residents in the [U.S. State Privacy Notice](#) section below. To the extent that there is a conflict between this Privacy Policy and the U.S. State Privacy Notice section, the U.S. State Privacy Notice section will control as to residents of those states. Please review this Privacy Policy carefully, especially before providing any Personally Identifiable Information through the Prodege Sites and Features or our Services. The

Prodege Sites and Features and our Services are generally operated in and controlled from the United States of America unless otherwise stated.

Prodege Sites and Features and our Services may collect and use location-aware and cross-device data for advertising and other purposes.

IF YOU DO NOT WISH TO HAVE US COLLECT, USE, AND SHARE INFORMATION AS DESCRIBED IN THIS PRIVACY POLICY, PLEASE DO NOT USE ANY OF THE PRODEGE SITES AND FEATURES OR OUR SERVICES.

Notice of Terms of Use, Including Arbitration: Your use of the Prodege Sites and Features and our Services is subject to our [Terms of Use](#), which includes binding individual arbitration of any disputes which may arise in connection with such use. Please note that your use of the Prodege Sites and Features or our Services constitutes your express agreement to our Terms of Use, including its arbitration provisions and class action waiver. Please read the Terms of Use—including the arbitration provisions—carefully, and do not use any of the Prodege Sites and Features or our Services if you do not agree.

Prodege, LLC and its Affiliates (defined below) (collectively, “**Prodege**,” “**we**,” “**our**” or “**us**”) own and operate a number of different services, including, without limitation, Swagbucks, MyPoints, InboxDollars, Upromise, CouponCause, Swagbucks Live, MyGiftCardsPlus, ySense, Tada, DailyRewards, Pollfish, BitBurst, Easy Bucks, AdGate Media, [Prodege.com](#), and others that may be added from time to time (collectively, the “**Prodege Sites**”). This Privacy Policy applies to the Prodege Sites and to all of the features, websites, mobile applications, Internet browser extensions, emails, online services and other functionalities (collectively, the “**Features**”) available via or related to the Prodege Sites, whether accessed via a computer, mobile device, or other devices you use (each a “**Device**” and collectively, “**Devices**”), or otherwise (collectively, the “**Prodege Sites and Features**”), the services available on or through the Prodege Sites and Features, including our emails and other electronic communications (collectively, “**our Services**”). Unless specifically stated, such as in the [U.S. State Privacy Notice](#) section, this Privacy Policy only covers information we collect through Prodege Sites and Features and our Services and does not cover any information we receive or collect offline or that is collected by any unrelated websites or companies to which we may provide links. Please contact us with any questions regarding this Privacy Policy and our privacy practices as instructed in Section 20 ([Contact Us](#)) of this Privacy Policy below.

2. Information We Collect Directly

When you visit any Prodege Sites and Features or use any of our Services, you may share and/or we may automatically collect information that identifies you personally. In

this Privacy Policy, **“Personally Identifiable Information”** (or **“PII”**) refers to any information that can reasonably be used to identify, contact or locate you; provided, however, that the [U.S. State Privacy Notice](#) section applies a definition of personal information under applicable state law that may be broader than PII. Examples of PII may include, without limitation, your name, your precise geo-location, your credit card number, your email address, your mailing address, and your phone number. We also collect, and may create from PII, information about you that is not PII (**“Non-PII”**). If we combine PII collected via Prodege Sites and Features or our Services with other of your PII or with Non-PII, that combined data will be treated as PII subject to this Privacy Policy.

PII and Non-PII may be collected on, through, or in connection with any of the Prodege Sites and Features or our Services. For example, we may collect PII and/or Non-PII when you create or register for an account with us, fill out surveys, join a mailing list, upload receipts, correspond with us, enter one of our sweepstakes or contests, choose to submit testimonials, stories, photos or the like, or otherwise volunteer or provide information about yourself. You may also choose to install and use optional Internet browser extensions, add-ons, or similar plug-in software and technologies (each an **“Extension”** and collectively, **“Extensions”**) which may collect and use your information in a variety of ways. For example, the Swagbucks SwagButton, MyPoints Score!, Tada, InboxDollars Billy Button, Upromise Extension, ySense Addon, and similar software or technologies we may offer from time to time are Extensions that allow you to shop directly with our merchant partners and qualify for rewards. The Extensions also provide other features and access to Offers (defined below), and allow you to monitor your earnings, customize your account information or experience, and other activities. If you install an Extension, we will automatically track certain websites you visit to allow us to provide the aforementioned features and to correlate your browser history, merchant visits, and Prodege Sites and Features engagements to provide better Services and Offers to you. In addition, Tracking Technologies (defined below) may be placed on your Devices when you install and use Extensions or when you click on an affiliate or Ad Network (defined below) link within a shopping-rewards feature. Your browsing activity on our merchant partners’ websites and other websites you visit may be tracked by cookies, Extensions, or other Prodege Sites and Features having such tracking capabilities. We may also use GPS or similar geo-location technology to determine the geo-coordinates of where you or your Device are located. In addition, our mobile applications may collect, among other things, certain information automatically, including, but not limited to the type of mobile Device you use, your mobile Device’s unique device identifier (**“UDID”**), the IP address of your mobile Device, your mobile operating system, the type of mobile Internet browsers you use, and information about the way you use the mobile application.

If you don't provide us with or allow us to collect your PII, we generally will be unable to provide you with our Services and you may be unable to use the Prodege Sites and Features.

You may be able to limit data collection by changing the settings on your Device (but our services and features may lose functionality as a result), or as otherwise explained in the sections below.

3. Information We Receive from Third Parties

We may also receive and supplement the information we directly collect from or about you with information from third parties, including Trusted Third Parties (defined below), and to the extent it is combined with PII collected via Prodege Sites and Features or our Services, it will be governed by this Privacy Policy. If you are on a third party website or service and you opt-in to receive information from us, the third party may forward to us your email address and other information about you so that we may contact you as requested. In addition, we may receive information from Third Party Services to ensure that you properly receive any qualified Offers and for our other Data Purposes (defined below). We may also supplement and combine the PII we collect about you with outside records from third parties in order to enhance our ability to provide you with Offers and for our other Data Purposes, and to the extent it is combined with PII collected via Prodege Sites and Features or our Services, it will be governed by this Privacy Policy.

4. Use and Sharing of Information

We use your PII and non-PII we collect about you in order to: (i) provide you with our Services; (ii) operate and improve the Prodege Sites and Features; (iii) provide advertising, content, surveys, location-based deals, special offers, promotions, and other rewards opportunities (collectively, "**Offers**"); and (iv) for other marketing, administrative, operational, business, and commercial purposes subject to applicable law and not inconsistent with this Privacy Policy or other notice by us at collection (collectively, our "**Data Purposes**"). We may use and disclose Non-PII for any purpose subject to applicable law and not inconsistent with this Privacy Policy or other notice by us at collection. Without limitation, your PII and non-PII may be used by itself, aggregated, or combined with unique identifiers (such as Prodege-assigned identifiers, UDIDs, etc.), and shared with (a) our parent companies, subsidiaries, sister companies, trusted agents and affiliated Services that we own and/or operate ("**Affiliates**"); and (b) our service providers, vendors, advertisers, merchants, survey partners, joint business ventures, and other trusted third parties (collectively, "**Trusted Third Parties**") (some of whom may offer Third Party Services (defined below)), for purposes related to our

business, including, without limitation, advertising, attribution, measurement of campaigns, analytics and research, and our other Data Purposes as permitted by applicable law. Notwithstanding the foregoing, no phone number you provide to us or one of our mobile service providers (currently Airship, Twilio, Telesign, and Button) for purposes of sending you a link for downloading a mobile app, special offer, a security verification, text (SMS) marketing, or otherwise, will be used or shared with any third party to be used for any other purpose, except as may be permitted or required by law or legal process or with your consent or at your direction.

5. Friend Referrals

We may provide you with an opportunity to invite your friends, family, and acquaintances ("**Friends**") to use our Services. If you elect to use our referral service for informing a Friend about any of our Services, you may provide us with your Friend's name and email address. Through our referral service, you may have the ability to direct us to automatically send the Friend one or more emails or other communications, on your behalf, inviting them to visit or register for our Services (which invite may include additional subsequent reminders and communications). You must have your Friend's consent to provide us with his or her information for this purpose and should not knowingly give us referral information for any person not permitted to use the Prodege Sites and Features, including, without limitation, a child under the age of 13, a person whose account has previously been suspended or deactivated, or a person who resides or is located in a territory where use of the Prodege Sites and Features is not authorized.

6. Community Features and User Content

The Prodege Sites and Features may provide you the opportunity to participate in, make available, and/or post text (e.g., questions, comments, and suggestions), images, audio, videos, or other content (collectively, "**User Content**") publicly through our blogs, chat rooms, forums, interactive features, public-facing member profile, third-party social networking services or other communication functionality ("**Community Features**"). Please note that certain information, such as your username, Service start date, earning preferences, qualified rewards, profile picture and other profile information we believe will help motivate you and others to participate in our program may be publicly displayed on the Prodege Sites and Features along with User Content. User Content may also contain metadata, which may contain information about or relating to you, that we may also collect, share and use. Anything posted through Community Features is publicly available. This means that others will have access to that User Content and may use it or share it with third parties; this is beyond our control. If you choose to voluntarily disclose PII in the User Content and/or on the

Community Features, that information will be considered publicly available information as well. The protections of this Privacy Policy will not apply to publicly available information. In addition, by posting through our Community Features, you are agreeing that we may use your User Content (and excerpts from your User Content) in connection with our Data Purposes.

7. Third Party Services

The Prodege Sites and Features contain links to, or otherwise enable the opportunity to interact with (e.g., Facebook button), other websites, and other services provided by Trusted Third Parties (such as when you link to their site to take a survey or transact with them to qualify for rewards) that we do not own, operate nor control (“**Third Party Services**”). In addition, because aspects of the Prodege Sites and Features include third-party Offers, Third Party Services may collect your information based on your interaction with those Offers, including via Tracking Technologies (defined and discussed below). In addition, by interacting with Offers via Prodege Sites and Features or our Services, you authorize and direct us to share your PII and non-PII with Third Party Services making Offers, and for them to share Offer-related activity data and other information with us. This helps us and them make and fulfill Offers, including making it easier for you to sign up for Offers, facilitating your communications or transactions with them, authenticating and/or validating your identification, crediting you with any qualified rewards, and for our other Data Purposes. Except as legally required for our service providers, the privacy and other practices of Third Party Services are not covered by this Privacy Policy, and we are not responsible for their privacy or other practices. We encourage our users to be aware of and to read the privacy statements, terms of service and similar disclosures and conditions of Third Party Services that collect PII or other data before visiting or otherwise interacting with those services.

For more information on Third Party Services, see sections 8, 9, 11 and 12 of this Privacy Policy ([Advertising Networks](#), [Session Replay and Analytics Companies](#), [Card Linked Offers Programs](#) and [Social Features](#)).

8. Advertising Networks

Companies that host networks connecting advertisers with delivery platforms for digital advertising (collectively, “**Ad Networks**”), which are Third Party Services, may provide advertising based on your interests, as reflected in your use of Prodege Sites and Features and our Services, as well as your use of other websites and services. Some of these Ad Networks may place persistent cookies or other Tracking Technologies (defined below) on your Devices, allowing them to recognize you and/or your Device each time they send you an online advertisement. Ads themselves may

also include Tracking Technologies. In this way, Ad Networks may compile information about where you see advertisements online and determine which ads you click on, so, for instance, that we and they may provide you with Offers or advertisements believed to be of most interest to you. We are not the data controller for the cookies or other Tracking Technologies that may be placed by these third parties on your Devices, nor do we have responsibility for these third parties' privacy policies or information collection practices. You may limit or remove such cookies and Tracking Technologies through your Device settings; for more information, visit section 10(ii) ([What Are My Cookie Choices?](#)) below.

9. Session Replay and Analytics Companies

We use certain third-party analytics and/or other technology providers to help us understand how you use Prodege Sites and Features or our Services, and these companies may set their own cookies and other Tracking Technologies on your Devices. For example, we may use third-party services to record and review your interactions with the Prodege Sites and Features and our Services, including mouse movements, clicks, page visits, keystrokes/key touches, and other details, including any PII that you provide. These "session replay" services help us organize and analyze your interaction data for our Data Purposes, including to improve and prevent fraud related to Prodege Sites and Features and our Services. By using any of the Prodege Sites and Features or our Services, you expressly consent to the recording and sharing of your PII and other data with third-party "session replay" services and other analytics providers.

We may also use Google Analytics and similar third-party analytics providers to track visitors' activity on our website. Google Analytics and similar third-party analytics providers may also use web browsing data and other data analysis to improve their own products. For more information on how to limit this activity, including to learn about the opt-out mechanism Google offers, visit section 10(ii) ([What Are My Cookie Choices?](#)) below. These and other Trusted Third Parties may collect information about you, including but not limited to your online activities over time and across different websites and services, when you use the Prodege Sites and Features or our Services, or other online websites and services.

10. Cookies and Tracking Technologies

i. Use of Cookies and Tracking Technologies

We set and access, and third parties (including Trusted Third Parties) may set and access, cookies, web beacons, embedded scripts, pixels, tags, software development kits ("SDKs"), session replay tools, and other tracking technologies (collectively, "**Tracking Technologies**") on your Devices in connection with your use of Prodege Sites

and Features or our Services. Such third parties ("**Cookie Operators**") may collect information across various channels using Tracking Technologies for purposes of delivering more relevant Offers to you or other Business Purposes. We may use a variety of Tracking Technologies in connection with our Data Purposes. Tracking Technologies may automatically capture PII and other information, including, without limitation, your IP Address, UDID, and browser or operating system type and version, and may detect whether your Device or software has certain capabilities such as a microphone or webcam access. We and Third Party Services generally use Tracking Technologies and the information they generate to support the Prodege Sites and Features and our Services or Third Party Services, including, for instance: (i) by offering you surveys, shopping, and other targeted Offers; (ii) for identity verification; (iii) for analytics; (iv) to ensure compliance with our programs; and (v) to identify and honor your choices (such as opt-outs). Tracking Technologies may also be used as follows: (a) to provide you with convenience when you access the Prodege Sites and Features or our Services by remembering that you have visited us before and by remembering your username, password and other user information, and your preferences to help you avoid future re-entry of certain information; (b) to allow us and Third Party Services to understand or predict your interests so we and they can personalize your experience on Prodege Sites and Features or our Services and elsewhere online, across Devices, web browsers, email, mobile and other applications. In doing so, we and Third Party Services may link the information collected from Tracking Technologies, and from other sources, with other of your PII and non-PII, and we and they may track your web-browsing and other activity in order to provide you with Offers and for our or their other Data Purposes); (c) for analytical and statistical purposes, quality control, validation and verification purposes, and to improve the services we and Third Party Services offer; and (d) Third Party Services may link the information we share with them (or that they collect) to cookies stored on your browser or Devices, and they may collect information such as your IP address, UDID, browser or operating system type and version, and demographic or inferred-interest information. Third Party Services may use this information to recognize you across different channels and platforms, including but not limited to, computers, mobile devices, and Smart TVs, over time for advertising, analytics, attribution, and reporting purposes. For example, Third Party Services may deliver an advertisement to you in your web browser based on a purchase you made in a physical retail store, or they may send a personalized marketing email to you because you visited a particular website. Our mobile applications may include Tracking Technologies that share your Device's precise geo-location and other details about your Device (like hardware characteristics, a variety of sensor data, and a list and history of installed third-party applications) with Third Party Services who may use this information to generate Offers for you, for advertising, attribution, measurement of campaigns, analytics, and research, and their or our other Data Purposes. See instructions to limit or disable such tracking in section 10(ii) below;

but be aware that limiting such tracking will affect some Device or mobile application functionality and may limit your ability to use our Services, complete Offers and earn rewards.

ii. What Are My Cookie Choices?

Cookies may include a small data file which is stored on your systems. We use both session cookies and persistent cookies. For the session cookies, once you close your browser, the cookie terminates. A persistent cookie is a small text file stored on your hard drive for an extended period of time. Persistent cookies can be removed or disabled by following your web browser help-file directions.

You can exercise control over browser-based cookies by adjusting the settings on your browser, and mobile Devices may offer ad and data limitation choices. Please note that when you use cookie control tools, you will have to change your settings for each browser and Device you use, and your limitation on cookies can limit the functionality of online services you use, including Prodege Sites and Features and our Services. Use the help function on your browser or click on the applicable links below to learn more:

- [Google Chrome](#)
- [Firefox](#)
- [Internet Explorer](#)
- [Edge](#)
- [Safari](#)

If you block cookies in this manner, Prodege Sites and Features and our Services (including the ability to complete Offers and earn rewards), may not operate as intended.

One use of cookies is interest-based advertising, which uses your activity information to help provide you with more relevant Offers. To learn more about internet-based advertising in general, and exercise certain opt-outs that some Ad Networks provide, which may include use of geo-location, cross-device data-directed, and/or “audience matched advertising” ads, please visit the following ad industry self-regulatory resources:

Digital Advertising Alliance (Web Browser Opt-Out)	US: http://www.aboutads.info/choices Canada: https://youradchoices.ca/en/tools
Digital Advertising Alliance (Mobile App Opt-Out)	US: http://www.aboutads.info/appchoices Canada: https://youradchoices.ca/en/tools

Network Advertising Initiative (Opt-Outs)	http://www.networkadvertising.org/managing/opt_out.asp
---	---

We support these self-regulatory programs and expect the Ad Networks we work with to do so as well. If you'd like to opt-out of being tracked by Google Analytics, simply install this add-on to your browser: <https://tools.google.com/dlpage/gaoptout>.

We are not responsible for the completeness, accuracy or effectiveness of any third-party cookie-choice programs or tools. If you exercise these choice controls they may need to be compiled on each browser and Device you use, and if they use a cookie to signal your opt-out, your choice may no longer be recognizable if you later clear or block cookies. Not accepting cookies (or opting out of cookies), installing ad blocking technologies, and/or disabling analytics providers may make certain features of the Prodege Sites and Features and our Services unavailable to you and may affect our ability to validate whether or not you qualified for a reward by successfully completing an Offer.

Note that your browser settings may allow you to automatically transmit a "Do Not Track" signal to websites and online services you visit. At present, we do not believe that there is a consensus among industry participants as to what "Do Not Track" means in this context. Like many websites and online services, we currently do not alter our practices when we receive a "Do Not Track" signal from a user's browser. To find out more about "Do Not Track," you may wish to visit <http://www.allaboutdnt.com>.

11. Card Linked Offers Programs

We may offer a service enabling you to enroll a qualifying payment card in order to earn rewards or benefits when you make qualifying transactions with participating merchants (a "**CLO Program**"). Your participation in a CLO Program is further governed by our [Card Linked Offer Service Terms](#). If you participate in a CLO Program and provide your payment information for that purpose, we and Third Party Services (including, without limitation, Braintree Payments (a division of PayPal, Inc.), Visa, Inc., Rewards Network, and Figg, Inc.) will have the right to use and share the transaction information generated in such CLO Program ("**CLO Transaction Data**") for the purposes of operating and improving the CLO Program, including, without limitation: (a) to confirm whether you qualify for an Offer; (b) to confirm whether a specific transaction occurred or rewards were earned (for example, the date and amount of your purchase and the last 4 digits of your card number so the merchant can verify your purchase if there is a missing or disputed transaction); (c) to allow participating merchants and others to assess the results of their campaign and analyze ways to improve or optimize a CLO Program and its Offers; (d) to create a record of the CLO

Transaction Data and thereafter maintain and use such CLO Transaction Data in connection with operating the CLO Program; and (e) to provide information in response to a request from a government authority or a payment organization involved in a transaction with you, a merchant, another relevant Trusted Third Party, or others. **By participating in a CLO Program, you authorize and direct the sharing, exchange, and use of CLO Transaction Data described above and herein by and among us and Third Party Services, applicable payment card networks, and participating merchants.** Please visit the Card Linked Offer Service Terms to learn more about the data collection, use, and sharing practices related to the CLO Program. If you would like to opt out of card linking and CLO Transaction Data collection in connection with a CLO Program, please visit the card linking section of the applicable Service and remove any payment cards that you no longer wish to be associated with the CLO Program.

12. Social Features

Certain functionality on Prodege Sites and Features or our Services may permit interactions that you initiate between our Services and third-party social media services ("**Social Media Services**") such as Google, Apple, Facebook, Pinterest, Instagram and Twitter ("**Social Features**"). Examples of Social Features include enabling you to "like" or "share" content from our Services with Social Media Services; to log-in to our Services using your username and password for Social Media Services; to transmit content to or from our Services to or from your account on Social Media Services; and to otherwise connect our Services to Social Media Services. Enabling or interacting with Social Features may also set one or more cookies or other Tracking Technologies on your Devices. Please refer to the terms of use and privacy policies of such Social Media Services offering such Social Features. If you choose to use Social Features, information you post or provide access to may be shared with and publicly displayed on our Services or on such Social Media Services. Similarly, if you post information on a Social Media Service that references any of our Services (e.g., by using a hashtag associated with any of our Services in a tweet or status update), your post may be published on the Prodege Sites and Features in accordance with the terms of the Social Media Services and our [Terms of Use](#). In addition, we may receive information about you if other users of a Social Media Service give us access to their profiles and you are one of their "connections," or information about you is otherwise accessible through your connections' web pages, profile pages, groups you or they belong to, or similar pages on such Social Media Service.

The information we collect in connection with Social Features is subject to this Privacy Policy. The information collected by any Social Media Service via Social Features remains subject to their privacy practices, including whether they continue to share

information with us, the types of information shared, and your choices with regard to what is visible to others on such Social Media Service.

13. Disclosure of Data

In addition to the types of disclosure and sharing of data described throughout this Privacy Policy, we may disclose your PII and non-PII as described in this section. We may disclose your PII and non-PII when required by law, or where we have a good-faith belief that such action is necessary to comply with a judicial or administrative proceeding, a criminal investigation, a court order, or legal process served on us. We may also share your PII and non-PII at the request of governmental authorities conducting an investigation, or if we in our sole discretion believe there to be a credible situation that requires us to investigate, prevent, or take action regarding illegal activities, suspected fraud or abuse, situations involving potential threats to the physical safety of any person, or violations of our Terms of Use or Privacy Policy for any of the Prodege Sites and Features or our Services. We may also use IP addresses, UDID or other Device, activity or session identifiers to identify users, and we reserve the right (in our sole discretion) to do so in cooperation with Third Party Services, as well as copyright owners, Internet service providers, wireless service providers, or law enforcement agencies, without notice to you. We may also share your PII with Third Party Services in connection with their performance of services to, or on behalf of, the Prodege Sites and Features or our Services (and vice versa) and for our Data Purposes. In addition, if you use our mobile applications, we may share your current geo-location with Third Party Services so that we or they may provide you with Offers based on your location, for our Data Purposes, and for advertising, attribution, measurement of campaigns, analytics and research. Please see section 15 ([Updating Your Information, Choice and Opt-Out](#)) below for information about how you can opt out of such sharing.

We may share or sell aggregate or individualized information about you that may include, without limitation: (1) your PII and related information; (2) your use of the Prodege Sites and Features and our Services; (3) Third Party Services and other websites you visit; and (4) your geo-location and information derived therefrom. We share this information with Trusted Third Parties for the purpose of providing you with Offers and for our Data Purposes.

14. Business Transactions

In the event Prodege or any of its Affiliates is involved with a business transition, such as a financing, merger, consolidation, restructuring, acquisition by another company, sale or assignment of rights or assets (or a portion thereof), or other company change, we may transfer your and other users' information, including PII and non-PII, and other

business data in connection with that business transaction (e.g., to a subsequent owner or operator of Prodege or any of our Services, or any affiliates, agents, service providers, or partners of the foregoing), including during the course of any due diligence process (collectively, “**Business Transactions**”).

15. Updating Your Information, Choice and Opt-Out

You are responsible for maintaining the accuracy of any information you submit to us, such as your contact information. If you have any questions about updating your information, privacy choices and/or opting out of certain programs, services, and data activities, please visit section 20 ([Contact Us](#)) below for more information and instructions to contact us. You may opt out of receiving marketing emails by: (i) following the opt-out instructions provided to you in those emails; (ii) visiting your account settings or similar features on the relevant Prodege Sites and Features; or (iii) contacting us as provided in section 20 ([Contact Us](#)) below. Please note that as long as you remain registered with or a user of any of the Prodege Sites and Features or our Services, even if you opt out of marketing emails, you may still receive administrative and transactional emails, such as notices about service and status updates and changes to our Terms of Use or Privacy Policy. If you sign up to receive text (SMS) messages from the Prodege Sites and Features, you may unsubscribe from any text SMS messages received by replying “STOP”. If you do not wish to receive advertisements, content, surveys, promotions, Offers, or rewards from us by virtue of your installation of our Extensions, you should not install or should uninstall such Extensions. You may remove or disable cookies and/or opt out of interest-based advertising as described above in section 10(ii) ([What Are My Cookie Choices?](#)) and you may clear your browser history in accordance with the system settings of your web browser. You may also opt out of providing your geo-location information to us by turning off the location services for your Device located in your account settings (if available) or in your Device settings. If you do not want our mobile applications to collect any PII or non-PII about you, you should uninstall the application using the standard uninstall procedures that may be available as part of your mobile Device or via the mobile application marketplace or network where you obtained the mobile application.

16. Notification of Privacy Policy Updates

We reserve the right to make changes to this Privacy Policy from time to time via updates. If we decide to make an update with material changes to this Privacy Policy, we will provide notice of the update by sending you an administrative email and/or posting links to the updated Privacy Policy in places on the Prodege Sites and Features deemed appropriate by us so our users are always aware of what PII and other

information we collect, how we use it, and under what circumstances it may be shared with others. Your continued use of any of the Prodege Sites and Features and our Services after delivery of the administrative email to you, or after the update links are posted, constitutes your acceptance of the updated Privacy Policy as to any continued use of the Prodege Sites and Features and our Services, including our future use of PII or other information previously or thereafter collected in accordance with the updated Privacy Policy. If you do not accept the changes, please immediately discontinue your use of any Prodege Sites and Features and our Services and close your account with us.

17. Children's Privacy

The Prodege Sites and Features and our Services are for general audiences, and we do not knowingly collect any personal information (as defined by the federal Children's Online Privacy Protection Act ("**COPPA**") from children younger than the age of 13. If you are under the age of majority (18 in most states and provinces), you should use the Prodege Sites and Features and our Services only with the permission and guidance of your parent or guardian. If you are under 13, you should not use our Service. If we learn that we have inadvertently collected personal information from a child younger than 13, we will take actions as required by COPPA.

If a California resident is known to us to be under 16 years of age, we will obtain any required expressed opt-in consent to any sale of their personal information collected by the Prodege Sites and Features or our Services, in accordance with the CCPA and applicable regulations thereunder. California minors also have certain rights to remove their own public posts on the Prodege Sites and Features. More information is included in section G ([Additional Notices for California Residents](#)) of the U.S. State Privacy Notice below.

18. Security

We maintain security measures in place to help protect against the loss, misuse and alteration of the PII and other information under our control. Please be advised, however, that the Internet and other technologies and communication channels are, by their nature, not entirely secure, and your PII and non-PII may therefore be subject to interception or loss which is beyond our reasonable control. While we strive to protect your PII and non-PII, we cannot ensure or warrant the security of any PII or non-PII you transmit to us or that we otherwise collect, and any transmission is done at your own risk. Accordingly, as permitted by applicable law, we assume no responsibility or liability for disclosure of your PII or non-PII due to errors in transmission, unauthorized third-party access, or other causes beyond our reasonable control.

19. Location of Processing and Applicable Law

Although we generally maintain our user data in the United States, it is possible that some of the data processing may occur outside of the United States, carried out by companies or individuals under contract with us. While the data protection laws of these countries may vary, we will make every reasonable effort to protect your PII in accordance with this Privacy Policy. By using the Prodege Sites and Features and our Services, you consent to this transfer of your PII and non-PII to any server used by Prodege or its service providers from time to time.

If you are not a resident of the United States or Canada, please consult the international version of our Privacy Policy [here](#) and be aware that data protection laws in the United States and Canada (as well as the legal procedures for courts, governmental authorities, and parties in civil litigation to obtain access to our user data) may differ substantially from the laws and procedures in your country of residence. In addition, if you submit your PII to us, you are consenting to the processing, storage, use and transfer of that PII within the United States as provided in this Privacy Policy.

The interpretation and application of this Privacy Policy shall be governed by the laws of the United States and the State of California without regard to its conflict of law provisions. Except as otherwise expressly provided in our [Terms of Use](#), your use of the Prodege Sites and Features or our Services are not intended to subject us to the laws or jurisdiction of any state, country or territory other than that of the United States and the State of California.

20. Contact Us

If you have any questions or concerns regarding this Privacy Policy or your use of any Prodege Sites and Features or our Services, please visit our Help Center or contact options (located or accessed from the applicable Prodege Sites and Features footer or from main menu options). For questions relating to our privacy practices (other than California residents making CCPA requests), please visit the [Privacy](#) section of the appropriate Help Center. If your question is not answered in the Help Center, you can submit a privacy-related request by submitting a ticket to our Customer Support team for the appropriate Service. To contact us by mail, send your correspondence to the following address and specify the Prodege Sites and Features or our Services you are using along with your request, question or concern:

Prodege, LLC, 8605 Santa Monica Blvd, PMB 36227, West Hollywood, California 90069-4109, Attention: Privacy

U.S. STATE PRIVACY NOTICE

This U.S. State Privacy Notice ("**Notice**") applies to "**Consumers**" as defined respectively under the California Consumer Privacy Act, as amended by the California Privacy Rights Act (together, the "**CCPA**"), the Colorado Privacy Act, Connecticut's Act Concerning Personal Data Privacy and Online Monitoring, Chapter 603A of the Nevada Revised Statutes, the Utah Consumer Privacy Act, and the Virginia Consumer Data Protection Act, and all laws implementing, supplementing, or amending the foregoing, including regulations promulgated thereunder, as well as any additional U.S. state privacy laws now or hereafter applicable to the Company (collectively, "**U.S. State Privacy Laws**"). Capitalized terms used but not defined in this Notice shall have the meanings given to them under the relevant U.S. State Privacy Laws or (if applicable) in other sections of our Privacy Policy.

Applicability:

- Section A of this Notice provides notice of our data practices, including our collection, use, disclosure, and sale of Consumers' personal information or personal data under relevant U.S. State Privacy Laws (collectively, "**PI**").
- Sections B-F of this Notice provide information regarding Consumer rights under applicable U.S. State Privacy Laws and how you may exercise them.
- Section G of this Notice provides additional information for California residents only.

For California residents, the term "Consumer" is not limited to data subjects acting as individuals regarding household goods and services and includes data subjects in a business-to-business context (e.g., as a service provider or customer, or an employee of a service provider or customer). This is not the case in the other states.

Non-Applicability, Human Resources: This Notice does not apply to our job applicants, current or former employees, or independent contractors ("**Personnel**") in connection with their PI collected in connection with such relationship with the Company; however, our California Personnel may obtain a separate privacy notice that applies to them by contacting our Human Resources department at hr@prodege.com.

A. Notice of Data Practices

The description of our data practices in this Notice covers the twelve (12) months prior to the Effective Date and will be updated at least annually. Our data practices may differ between updates to this Notice; however, if materially different from this Notice,

we will provide supplemental pre-collection notice of the current practices, which may include references to other privacy policies, notices, or statements. Otherwise, this Notice serves as our notice at collection.

We may receive or collect your PI directly from you or from your Devices, from Third Party Services, or from other individuals and businesses, as well as public sources of data.

Generally, we Process your PI to provide you our Services and as otherwise related to the operation of our business, including for one or more of the following Business Purposes: Performing Services; Managing Interactions and Transactions; Security; Debugging; Providing Advertising & Marketing Services; Quality Assurance; Processing Interactions and Transactions; and Research and Development. We may also use PI for other Business Purposes in a context that is not a Sale or Share under applicable U.S. State Privacy Laws, such as disclosing it to our Service Providers, Contractors, or Processors that perform services for us ("**Vendors**"), to you, or to other parties at your direction or through your action (e.g., Third Party Services that you interact with in response to Offers); for the additional purposes explained at the time of collection (such as in the applicable privacy policy or notice); as required or permitted by applicable law; to the government or private parties to comply with law or legal process; and in Business Transactions (collectively, "**Additional Business Purposes**"). Subject to restrictions and obligations under U.S. State Privacy Laws, our Vendors may also use your PI for Business Purposes and Additional Business Purposes and may engage their own vendors to enable them to perform services for us.

We may also use and disclose your PI under this Notice for Commercial Purposes, which may be considered a "Sale" or "Share" under applicable U.S. State Privacy Laws, such as when Trusted Third Parties collect your PI via third-party cookies, and when we Process PI for certain advertising purposes. In addition, we may make your PI available to third parties for their own use via third-party cookies or otherwise.

As permitted by applicable law, we do not treat deidentified data or aggregate consumer information as PI and we reserve the right to convert, or permit others to convert, your PI into deidentified or aggregate consumer information, and may elect not to treat publicly available information as PI. We have no obligation to re-identify information or keep it longer than we need it to respond to your requests. Data exempt from U.S. State Privacy Laws are not included in this Notice.

We provide more detail on our data practices in the two charts that follow.

i. PI Collection, Disclosure, and Retention – By Category of PI

We collect, disclose, and retain PI as follows:

Category of PI	Examples of PI Collected and Retained	Categories of Recipients
1. Identifiers	This may include, but is not limited to: a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver's license number, or other similar identifiers.	Business Purpose Disclosure: <ul style="list-style-type: none"> • Service Providers (e.g., data processors, IT service providers, storage vendors, marketing service providers, security providers, and professional advisors) • Affiliates • Government entities (where we are under a duty to disclose or to protect our rights or the rights of others) • Other parties within the limits of Additional Business Purposes (e.g., when you engage
2. Personal Records	This may include, but is not limited to: physical characteristics or description, signature, telephone number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information.	
3. Personal Characteristics or Traits	This may include, but is not limited to: age, gender, nationality, race, or information related to medical conditions.	
4. Customer Account Details/ Commercial Information	This may include but is not limited to: records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.	
5. Internet Usage Information	This may include, but is not limited to: browsing history, search history, and information regarding your interaction with an Internet Web site, application, or advertisement.	
6. Geo-location Data	This may include, but is not limited to: precise physical location or movements and travel patterns.	
7. Sensory Data	This may include, but is not limited to: audio recordings of customer care calls, electronic, visual, thermal, olfactory, or similar information.	
8. Professional or Employment Information	This may include, but is not limited to: professional, educational, or employment-related information	

Category of PI	Examples of PI Collected and Retained	Categories of Recipients
9. Inferences from PI Collected	This may include, but is not limited to: creating a profile about a Consumer reflecting the Consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.	in Offer actions with Third Party Services)
10. Sensitive PI	Precise Geo-location (any data that is derived from a device and that may locate a consumer within a geographic area with a radius of 1,850 feet or less)	Sale/Share: <ul style="list-style-type: none"> • Cookie Operators (only to the extent such data is collected by a cookie or other Tracking Technology) • Licensees
	Sensitive Personal Characteristics (e.g., racial or ethnic origin, religious or philosophical beliefs, citizenship or immigration status, or union membership)	
	Health Information (PI collected and analyzed concerning a consumer's health, medical history, mental or physical health, diagnosis/condition, and medical treatment)	
	Sex Life / Sexual Orientation (PI collected and analyzed concerning a consumer's sex life or sexual orientation)	
	Financial Data (e.g., a consumer's account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account)	Business Purpose Disclosure: <ul style="list-style-type: none"> • Service Providers (e.g., data processors, IT service providers, storage vendors, marketing service providers, security providers, and
	Government Issued Identification Numbers (e.g., social security, driver's license, state identification card, or passport number)	
	Communication Content (e.g., the contents of a consumer's mail, email, and text messages, unless the business is the intended recipient of the communication)	

Category of PI	Examples of PI Collected and Retained	Categories of Recipients
		<p>professional advisors)</p> <ul style="list-style-type: none"> • Affiliates • Government entities (where we are under a duty to disclose or to protect our rights or the rights of others) • Other parties within the limits of Additional Business Purposes (e.g., when you engage in Offer actions with Third Party Services) <p>Sale/Share:</p> <ul style="list-style-type: none"> • None

We retain your PI based on how long we believe we have a legitimate purpose for the retention. In general, we retain all categories of PI listed in the chart above for as long as a customer account is open and for an additional 3 years after the account is closed; however, some data may be retained for a shorter or longer period. When deciding how long to keep your PI, we consider (among other things) whether we have an active relationship with you, whether we need to retain the PI to provide you our Services, whether we are subject to any legal obligations (e.g., any contracts or laws that require us to maintain certain data for a certain period of time), our Data Purposes, and our

Business Purposes and Additional Business Purposes. Rather than delete your PI, we might deidentify it by removing identifying details so it is no longer considered PI, in which event we will not attempt to re-identify that data.

There may be additional information we collect that meets the definition of PI under applicable U.S. State Privacy Laws but is not reflected by a category above, in which case we will treat it as PI as required but will not include it when we describe our practices by PI category.

ii. PI Use and Disclosure – By Processing Purpose

We use and disclose PI for the processing purposes described below. For the categories of recipients for each purpose, please refer to the chart above at Section A(i) (PI Collection, Disclosure, and Retention – By Category of PI), as indicated by relevant category of PI below:

Processing Purpose(s)	Example(s) of Processing Purpose	Categories of PI Implicated
1. Performing Services	<u>Provide our Services</u> : to provide you with Prodege Sites and Features and our Services, including Offers <u>Enable additional features</u> : to provide you with additional Prodege Sites and Features and enhance our Services <u>Process orders</u> : to process or fulfil an order or transaction <u>Contact You</u> : to contact and communicate with you about your use of our Services, including changes to our Services or our Services' policies <u>Account management</u> : to process your registration with our Services, verify your info is active and valid, and otherwise manage your account <u>Customer Service</u> : to respond to any questions, comments, or requests you have for us or for other customer service purposes <u>Payment and other purchase-related purposes</u> : to facilitate a purchase made using our Services, including payment processing	Identifiers, Customer Account Details/Commercial Information, Internet Usage Information, Geo-location Data, Sensory Data, Inferences

Processing Purpose(s)	Example(s) of Processing Purpose	Categories of PI Implicated
	<u>Other</u> : marketing, administrative, operational, business, and commercial purposes subject to applicable law and not inconsistent with this Privacy Policy or other notice by us at collection	
2. Managing Interactions and Transactions	<u>Auditing</u> : related to counting ad impressions to unique visitors, verifying positioning and quality of ad impressions, and auditing compliance with user interaction or transaction specifications and standards	Identifiers, Customer Account Details/Commercial Information, Internet Usage Information
3. Security	<u>Security/fraud prevention</u> : to protect the security of Company, our Services, and its users and to prevent and address fraud and violations of our terms and policies	Identifiers, Internet Usage Information, Customer Account Details/Commercial Information
4. Debugging	<u>Repairs</u> : identify and repair errors that impair existing intended functionality of our Services	Identifiers, Internet Usage Information, Customer Account Details/Commercial Information
5. Providing Advertising & Marketing Services	<u>Content and offers customization</u> : to customize your experience on our Services, or to serve you specific content and Offers that are relevant to/customized for you <u>Advertising, marketing, and promotions</u> : to assist us in determining relevant Offers; to develop and evaluate marketing and advertising campaigns; and for promotional activities, such as running sweepstakes, contests, and other promotions.	Identifiers, Internet Usage Information, Customer Account Details/Commercial Information, Geo-location Data, Inferences
6. Quality Assurance	<u>Quality and Safety of Service</u> : undertaking activities to verify or maintain the quality or safety of our Services, and to improve, upgrade, or enhance our Services	Identifiers, Internet Usage Information, Customer Account Details/Commercial Information, Geo-location Data, Inferences

Processing Purpose(s)	Example(s) of Processing Purpose	Categories of PI Implicated
7. Processing Interactions and Transactions	<u>Short-term, transient use</u> : including, but not limited to, non-personalized advertising shown as part of a Consumer's current interactions related to your use of our Services	Identifiers, Internet Usage Information, Customer Account Details/Commercial Information, Geo-location Data, Sensory Data, Inferences
8. Research and Development	<u>Research and analytics</u> : to better understand how Consumers access and use our Services, both on an aggregated and individualized basis, to improve our Services and respond to user preferences, and for other research and analytical purposes <u>Market research and customer satisfaction surveys</u> : to administer surveys and questionnaires, such as for market research or customer satisfaction purposes	Identifiers, Internet Usage Information, Customer Account Details/Commercial Information, Geo-location Data, Inferences
9. Additional Business Purposes	<u>Compliance with legal obligations</u> : to comply with legal obligations, as part of our general business operations, and for other business administration purposes <u>Prevention of illegal activities, fraud, injury to others, or violation of our terms and policies</u> : to investigate, prevent or take action if someone may be using info for illegal activities, fraud, or in ways that may threaten someone's safety or violate of our terms or policies <u>Purposes disclosed at PI collection</u> : We may provide additional disclosures at the time of PI collection, such as on an Offer page <u>Related or compatible purposes</u> : for purposes that are related to and/or compatible with any of the foregoing purposes	Identifiers, Personal Records, Personal Characteristics or Traits, Customer Account Details/Commercial Information, Internet Usage Information, Geo-location Data, Sensory Data, Professional or Employment Information, Inferences

Processing Purpose(s)	Example(s) of Processing Purpose	Categories of PI Implicated
10. Commercial Purposes	We may collect and use your PI for commercial purposes such as for interest-based advertising and sharing PI in a manner that is deemed a sale under the CCPA or other applicable U.S. State Privacy Laws.	Identifiers, Personal Records, Personal Characteristics or Traits, Customer Account Details/Commercial Information, Internet Usage Information, Geo-location Data, Sensory Data, Professional or Employment Information, Inferences

B. Your Consumer Rights and How to Exercise Them

We provide Consumers the privacy rights described in this section pursuant to the requirements of their applicable state's law, provided any such request meets the requirements for a Verifiable Consumer Request (defined below). For residents of states without applicable U.S. State Privacy Laws, we may consider requests under this section but will apply our discretion in whether and how we process them. We may also apply state law rights in states with U.S. State Privacy Laws prior to the effective date of such laws in our discretion.

To submit a request to exercise your Consumer privacy rights under U.S. State Privacy Laws, or to submit a request as an authorized agent, please follow the instructions at our Consumer Rights Request page [here](#) or mail your request to the following address: Prodege, LLC, 8605 Santa Monica Blvd, PMB 36227, West Hollywood, California 90069-4109, Attention: Privacy, and respond to any follow-up inquiries we make. Please be aware that we do not accept or process requests through other means (via phone, fax, chats, social media, etc.). More details on the request and verification process are provided in Section C ([How We Process Your Consumer Privacy Requests](#)) below. The Consumer rights we accommodate are as follows:

i. Right to Limit Sensitive PI Processing

With regard to PI that qualifies as Sensitive PI under U.S. State Privacy Laws, if you elect to provide us with that Sensitive PI, you will have consented to our collection and processing of such Sensitive PI. You may submit an opt-out request [here](#). However, under applicable U.S. State Privacy Laws, you can limit certain Sensitive PI Processing

with the exception of the following processing purposes or any other permitted purposes under such U.S. State Privacy Laws:

- To perform our Services at your request or at your direction;
- To prevent, detect, and investigate security incidents, fraudulent activity, illegal actions, etc.;
- For short term transient use, including, but not limited to, non-personalized advertising as part of your interaction with our Services; and
- To maintain or service accounts, provide customer service, process or fulfill Offers, orders and transactions, verify customer information, process payments, or provide similar services.

ii. Right to Know/Access

Residents of California, Colorado, and Virginia are entitled to access PI maintained by the Company up to twice in a 12-month period. Residents of Connecticut and Utah are entitled to access PI maintained by Company once in a 12-month period, with subsequent requests subject to a service fee.

a) Categories (available for California Residents only)

California residents have a right to submit a request for any of the following for the period that is 12-months prior to the request date:

- The categories of PI we have collected about you.
- The categories of sources from which we collected your PI.
- The Business Purposes or Commercial Purposes for our collecting or Selling your PI.
- The categories of third parties to whom we have shared your PI.
- A list of the categories of your PI disclosed for a Business Purpose and, for each, the categories of recipients, or that no disclosure occurred.
- A list of the categories of your PI sold and, for each, the categories of recipients, or that no sale occurred.

b) Specific Pieces (Transportable Copies)

You may request to confirm if we are Processing your PI and, if we are, to obtain a transportable copy of your PI that we have collected and are maintaining, as required by applicable U.S. State Privacy Laws. If you wish to receive specific pieces of your PI, we will attempt to honor requests for specific pieces of your PI where reasonably possible. We have no obligation to re-identify information or to keep PI longer than we

normally retain it or longer than we are required to under applicable law to comply with access requests.

iii. Do Not Sell / Share / Target for Advertising

Various U.S. State Privacy Laws have broad and differing concepts of “Selling” PI for which an opt-out is required, with some states including PI transfers for non-monetary consideration and other states only including PI transfers for monetary consideration. California also has an opt-out from “Sharing” for Cross-Context Behavioral Advertising purposes (use of PI from different businesses or services to target advertisements across websites or apps). Other states have an opt-out of “Targeted Advertising” (defined differently, but also addressing tracking, profiling, and targeting of advertisements). We may Sell or Share your PI and/or use your PI for Targeted Advertising, as these terms apply under U.S. State Privacy Laws. However, we provide you with an opt-out of Sale/Sharing/Targeting that is intended to combine all of these various state opt-outs into a single opt-out available regardless of which U.S. State Privacy Law is applicable to your PI.

Ad Networks and other Trusted Third Parties may associate cookies and other Tracking Technologies that collect PI about you on Prodege Sites and Features or in connection with our Services, or otherwise Collect and Process PI that we make available about you. We understand that making your PI available on Prodege Sites and Features or in connection with our Services, or otherwise, to Trusted Third Parties could be deemed a Sale and/or Share under some U.S. State Privacy Laws and thus we will treat such PI (e.g., cookie ID, IP address, and other online IDs and internet or other digital activity information) collected by Trusted Third Parties that are not limited to acting as our Service Provider (or Contractor or Processor), as a Sale and/or Share and subject to your right to make a Do Not Sell/Share/Target opt-out request. We will not Sell your PI, Share your PI for Cross-Context Behavioral Advertising, or Process your PI for Targeted Advertising if you make a Do Not Sell/Share/Target opt-out request as follows:

Opt-out for non-cookie PI: If you want to limit our Processing of your non-cookie PI (e.g., your email address or web browsing activity) for Targeted Advertising, or opt-out of the Sale/Sharing of such PI, you may make an opt-out request [here](#).

Opt-out for cookie PI: If you want to limit our Processing of your cookie-related PI for Targeted Advertising, or opt-out of the Sale/Sharing of such PI, you may exercise an opt-out request by following the instructions on our Consumer Rights Request page [here](#), or by clicking the link to update [Your Cookie Choices](#). This cookie management tool enables you to exercise such an opt-out request and enable certain cookie preferences on your Device. Since your browser opt-out is designated by a cookie, if you clear or block cookies on your Device, your preferences may no longer be effective, and you will need to enable them again via our cookie management tool.

Opt-out preference signals ("OOPS", as they are known in California; also known as global privacy control or GPC): Some of the U.S. Privacy Laws require businesses to process OOPS or GPC signals, which are signals sent by a platform, technology, or mechanism, enabled by individuals on their devices or browsers, that communicate the individual's choice to opt-out of the Sale and Sharing of PI. To use an OOPS/GPC, you can download a compatible internet browser or a plugin for on your current internet browser and follow the settings to enable to OOPS/GPC. We have configured the settings of our consent management platform to receive and process OOPS/GPC signals on our website, as explained by our consent management platform [here](#). We process OOPS/GPC signals with respect to any Sales and Sharing of PI with Trusted Third Parties that may occur via cookies or other Tracking Technologies, as discussed above and apply it to the specific browser on which you enable OOPS/GPC. We do not: (1) charge a fee for use of our service if you have enabled OOPS/GPC; (2) change your experience with any product or service if you use OOPS/GPC, although it may affect our ability to accurately track your activities for crediting your account with qualified rewards; or (3) display a notification, pop-up, text, graphic, animation, sound, video, or any interstitial in response to the OOPS/GPC, except for indicating whether we recognize the signal.

We may disclose your PI for the following purposes, which are not a Sale or Share: (i) if you direct us to disclose PI; (ii) to comply with a Consumer rights request you submit to us; (iii) disclosures amongst the entities that constitute Company as defined above, or as part of a Business Transaction; and (iv) as otherwise required or permitted by applicable law.

iv. Right to Delete

Except to the extent we have retention rights under applicable law, you may request that we delete your PI. Our retention rights include, without limitation:

- To complete transactions and services that you have requested;
- For security purposes;
- For legitimate internal Business Purposes (e.g., maintaining business records);
- To comply with law and to cooperate with law enforcement; and
- To exercise or defend legal claims.

Please also be aware that making a deletion request does not ensure complete or comprehensive removal or deletion of PI or content you may have posted.

Under certain U.S. State Privacy Laws, your deletion right may apply only to PI that we collected directly from you.

v. Correct Your PI

Consumers may bring inaccuracies they find in their PI that we maintain to our attention, and we will act upon such a report as required by applicable law.

You can also make changes to your PI in your online account in the account settings section of the account. That will not, however, necessarily change your PI in other places where we may maintain it.

C. How We Process Your Consumer Privacy Requests

To submit a request to exercise your Consumer privacy rights, or to submit a request as an authorized agent, please follow the instructions at our Consumer Rights Request page [here](#) or mail your request to the following address: Prodege, LLC, 8605 Santa Monica Blvd, PMB 36227, West Hollywood, California 90069-4109, Attention: Privacy, and respond to any follow-up inquiries we make. In addition, you may email privacyrequest@prodege.com and we will respond with the appropriate web submission form for you to use for the submission of your request. To submit a Do Not Sell/Share/Targeting Request for cookie-related PI or the right to limit Sensitive PI processing, click [here](#). Please be aware that we do not accept or process requests through other means (via phone, fax, chats, social media, etc.).

i. Your Request Must be a Verifiable Consumer Request

As permitted or required by applicable U.S. State Privacy Laws, any request you submit to us must be a **Verifiable Consumer Request**, meaning that when you make a request, we may ask you to provide verifying information, such as your name, e-mail, phone number and/or account information. We will review the information provided and may request additional information (e.g., transaction history) to ensure we are interacting with the correct individual. We will not fulfill your Right to Know (Categories), Right to Know (Specific Pieces), Right to Delete, or Right to Correction request unless you have provided sufficient information for us to reasonably verify you are the Consumer about whom we collected PI. We do not verify opt-outs of Sell/Share/Target or Limitation of Sensitive PI requests unless we suspect fraud.

You are not required to create a password-protected account with us to make a Verifiable Consumer Request, but you may use your password-protected account to do so. If we suspect fraudulent or malicious activity on or from the password-protected account, we may decline a request or request that you provide further verifying information.

We verify each request as follows:

- Right to Know (Categories) (available for California residents only): If you do not have a password-protected account, we verify your Request to Know Categories of PI to a reasonable degree of certainty, which may include matching at least two data

points provided by you with data points maintained by us, which we have determined to be reliable for the purpose of verifying you. If we cannot do so, we will refer you to this Notice for a general description of our data practices.

- *Right to Know (Specific Pieces)*: If you do not have a password-protected account, we verify your Request To Know Specific Pieces of PI to a reasonably high degree of certainty, which may include matching at least three data points provided by you with data points maintained by us, which we have determined to be reliable for the purpose of verifying you together with a signed declaration under penalty of perjury that you are the Consumer whose PI is the subject of the request. If you fail to provide requested information, we will be unable to verify you sufficiently to honor your request, but we will then treat it as a Right to Know Categories Request if you are a California resident.
- *Do Not Sell/Share/Target & Limit Sensitive PI*: No specific verification required unless we suspect fraud.
- *Right to Delete*: If you do not have a password-protected account, we verify your Request to Delete to either (i) a reasonable degree of certainty, which may include matching at least two data points provided by you with data points maintained by us, or (ii) a reasonably high degree of certainty, which may include matching at least three data points provided by you with data points maintained by us, depending on the sensitivity of the PI and the risk of harm to the Consumer posed by unauthorized deletion. If we cannot verify you sufficiently to honor a deletion request, you can still make a Do Not Sell/Share/Target and/or Limit Sensitive PI request.
- *Correction*: If you do not have a password-protected account, we verify your Request to Correct PI to either (i) a reasonable degree of certainty, which may include matching at least two data points provided by you with data points maintained by us, or (ii) a reasonably high degree of certainty, which may include matching at least three data points provided by you with data points maintained by us, depending on the sensitivity of the PI and the risk of harm to the Consumer posed by unauthorized correction.

To protect Consumers, if we are unable to verify you sufficiently, we will be unable to honor your request. We will use PI provided in a Verifiable Consumer Request only to verify your identity or authority to make the request and to track and document request responses, unless you also gave it to us for another purpose.

ii. Agent Requests

Authorized agents may exercise rights on behalf of California Consumers, but we reserve the right to also verify the Consumer's identity directly as described above. Authorized agents must contact us by submitting a request through our Consumer Rights Request page [here](#) and indicating in the open text field that they are submitting the request as an agent. We will require the agent to demonstrate authority to act on behalf of the Consumer by providing, for example, evidence of the agent's identity, proof of registration with the California Secretary of State (if the agent is a business), and at least one of the following evidencing proof of the agent's legal authority to act on behalf of the individual Consumer: (i) presenting a Power of Attorney granted under the Probate Code that we can reasonably verify; or (ii) signed permission by the Consumer.

We may also require the Consumer to verify their own identity directly with us and to directly confirm with us that they provided the authorized agent permission to submit the request.

In addition, residents of Colorado and Connecticut may use an agent to make an opt-out request subject to reasonable verification of agent authority and consumer identity.

In the absence of any of the general conditions detailed above, we are entitled to reject any request submitted through an agent. In addition, the agent is subject to the verification standards applicable to the type of request(s) made.

iii. Appeals (Colorado, Connecticut, and Virginia residents only)

If you are a resident of Colorado, Connecticut, or Virginia, you may appeal Company's decision regarding a request by contacting us at privacyappeals@prodege.com with the following subject line: "CRR Appeals Request".

iv. Our Responses

Some PI that we maintain is insufficiently specific for us to be able to associate it with a Consumer (e.g., clickstream data tied only to a pseudonymous browser ID). We do not include that PI in response to those requests. If we deny a request, in whole or in part, we will explain the reasons in our response.

We will make commercially reasonable efforts to identify Consumer PI that we Process to respond to your Consumer request(s). In some cases, particularly with voluminous and/or typically irrelevant data, we may suggest you receive the most recent or a summary of your PI and give you the opportunity to elect whether you want the rest. We reserve the right to direct you to where you may access and copy responsive PI yourself. We may also refuse to act upon a request that is excessive, repetitive, unfounded, or overly burdensome.

Consistent with applicable U.S. State Privacy Laws and our interest in the security of your PI, we will not deliver to you your Social Security number, driver's license number, or other government-issued ID number, financial account number, an account password, or security questions or answers, in response to a Consumer privacy rights request; however, you may be able to access some of this information yourself through your account if you have an active account with us.

D. Non-Discrimination/Non-Retaliation

We will not discriminate or retaliate against you in a manner prohibited by applicable U.S. State Privacy Laws for your exercise of your Consumer privacy rights. We may charge a different price or rate, or offer a different level or quality of good or service, to the extent that doing so is reasonably related to the value of the applicable data.

E. Notice of Financial Incentive Programs

We may offer rewards or other benefits ("**Incentives**") from time-to-time to Consumers that provide us with PI, such as name, phone number, e-mail address, IP address, or geo-location. You may opt-in to Incentives by subscribing to our [Incentive programs we may offer from time-to-time. If you subsequently wish to withdraw from such programs, the method for doing so will be explained in the program Terms of Use, and you may do so at any time. For more information, including valuation notice, see our Notice of Financial Incentives [here](#).

F. Our Rights and the Rights of Others

Notwithstanding anything to the contrary, we may collect, use and disclose your PI as required or permitted by applicable law and this may limit or affect your rights under U.S. State Privacy Laws. In addition, we are not required to honor your requests to the extent that doing so would infringe upon our or another person's rights or conflict with applicable law.

G. Additional Notices for California Residents

This Notice provides additional information on our online practices and the rights of California residents related to Prodege Sites and Features and our Services.

i. **California Minors Erasure**

If you are a California resident under eighteen (18) years of age who has posted content or information on Prodege Sites and Features or our Services, you can request

removal by contacting us at the mailing address set forth in the [Contact Us](#) section above detailing where the content or information is posted and attesting that you posted it. We will then make reasonably good faith efforts to remove the post from prospective public view or anonymize it so you cannot be individually identified to the extent required by applicable law. This removal process cannot ensure complete or comprehensive removal. For instance, third parties may have republished or archived content by search engines and other means that we do not control.

ii. Affirmative Opt-In for Sale or Sharing of PI of California Residents Under 16 Years of Age

We do not knowingly Sell or Share the PI of California residents under the age of sixteen (16), unless we receive affirmative opt-in authorization from (i) the under-16 California resident if he or she is at least 13 years of age, or (ii) the parent or guardian of the California resident if he or she is less than 13 years of age. If you think we may have unknowingly Sold or Shared PI of a California resident under 16 years of age without the appropriate affirmative opt-in authorization, please report that to us as described in the [Contact Us](#) section above.

iii. Shine the Light

We provide California residents with the option to opt-out to sharing of “personal information,” as defined by California’s “Shine the Light” law, with third parties (other than with Company affiliates) for such third parties own direct marketing purposes. California residents may exercise this opt-out, request information about our Shine the Light law compliance, and/or obtain a disclosure of third parties we have shared information with and the categories of information shared. California residents may make such a request, or inquire further about our compliance with this law, by emailing privacyrequest@prodege.com or mailing us at the address set forth in the [Contact Us](#) section above. You must put the statement “Shine the Light Request” in the body of your correspondence. In your request, please attest to the fact that you are a California resident and provide a current California address for your response. This right is different than, and in addition to, CCPA rights, and must be requested separately. We are only required to respond to one request per person each year. We are not required to respond to requests made by means other than through the provided e-mail address or mailing address (requests by phone, fax, chats, social media, etc.). We are not responsible for requests that are incomplete or not labeled and sent properly.

- [Terms of Use](#)
- [Privacy Policy](#)



QUEST
MINDSHARE™

PRIVACY POLICY





Privacy Policy

Your Privacy

Quest Global Research Group Inc. (“**Quest**”) is committed to respecting the privacy of survey respondents and other online users of Quest's services. Quest's Privacy Policy governs the collection, use, retention and security of information gathered from survey respondents and other online users of Quest's services.

Quest does not disclose any personally identifiable information (“**Personally Identifiable Information**” or “**PII**”) about survey respondents to third parties, except in reporting the survey responses to those of Quest's clients commissioning such surveys or as required by law. PII means information that individually identifies you, such as your name, address, or email address.

Consent

Your consent is the most important part of any transaction involving both the information you’ve previously provided Quest and any requests for information.

Quest will never disclose any non-aggregated and non-anonymized information you’ve previously provided us without explicit consent from you regarding the release of that information to another individual/company/organization. By non-aggregated and non-anonymized information we mean the specific information you’ve provided as opposed to a depersonalized data set that uses your information as part of the whole dataset in a manner that doesn’t provide any personal identification.

Requests for your PII will generally be preceded by messaging that informs you of this request, its purpose, and the proposed use(s), so you can decide if you want to provide consent.

You have the right to know how the information you provide is being used. Before you consent to providing PII, you have the right to know about any entities or organizations that can access the PII you provide.

Collected Information

Quest collects a wide range of information about survey respondents depending on the information needs of our surveys. For example, survey respondents may be requested to provide certain personally identifiable, financial or demographic information, as well as specific opinions about a variety of goods and services. Responses to all survey questions are completely voluntary. A survey respondent should only provide responses to questions they are comfortable answering and survey respondents may decline to answer any survey question.

Quest reserves the right to report information gathered through the survey (e.g., demographic data, preferences, etc.) to Quest's clients commissioning such surveys. Further, you acknowledge and agree that any information you voluntarily disclose in the survey may be provided to the commissioner of the survey. Quest does not disclose a survey respondent's personally identifiable information to anyone unless the survey respondent has consented to such disclosure or a disclosure is required by law.

You have the right to the information and data you have provided Quest. You may request a copy of the information and data you provide, and Quest will provide a copy of your information to you in a timely manner, subject to exceptions under applicable law.

Additional Information From Survey Respondents

Quest's servers may automatically recognize data relating to a survey respondent, which may include a respondent's domain name, IP addresses, location data, or other information about a respondent's internet connection ("**Meta Data**").

Quest may gather anonymous "Traffic Data" that does not personally identify a survey respondent but that may be helpful for improving the services Quest offers. "**Traffic Data**" can include the full Uniform Resource Locators (URLs), clickstream to, through and from our website (including date and time), page response times, download errors, length of visits to certain pages, page interaction information (such as scrolling, clicks, and mouse-overs) and methods used to browse away from Quest's website.

Quest may also use cookies on our platform to help us provide panelists with a better experience and to provide quality control and validation functions. You can choose whether to accept cookies by changing the settings on your browser. However, if you choose to disable this function, your experience at our website may be diminished and some features may not work as they were intended.

Quest may use and gather any Meta Data, Traffic Data or any other data that is not PII, which you have provided to Quest (collectively, “**User Content**”).

Opt-Out

You have the right to opt out of information request at any time. This means that even though you’ve previously given consent to the collection and use of your information, you can subsequently decide that you want any portion of the information you’ve provided to no longer be used by Quest.

Quest also honors respondents' requests to be excluded from marketing solicitations and, as dictated by the applicable laws, only sends such messages if requisite implied or express consents have been obtained. To be removed from this mailing list, simply email your request to info@questmindshare.com.

Protecting Respondent Information

Quest is committed to handling the personally identifiable information and data of survey respondents with care, integrity and in accordance with applicable laws. Quest uses industry standard security practices to protect such information and data. However, regardless of the security protections and precautions Quest undertakes, there is always a risk that personal data may be viewed and used by unauthorized third parties. Should an unauthorized third party breach Quest’s security measures, Quest will follow all applicable procedures related to breach reporting and remediation.

Disputes Concerning Privacy Policy

If you have any complaint concerning how Quest has handled your personal information, please contact Quest using the contact information described below. Quest will comply with all applicable laws and make every reasonable effort to address and resolve your concerns.

Compliance

By signing up to and participating in a Quest panel, you agree to Quest's privacy policy and any other related terms of use. If you do not agree with our policies and practices, your choice is not to use our website or participate in a Quest panel.

Contact Quest

If you have questions about this Privacy Policy, Quest's practices related to the handling of data from survey respondents, or if you would like to have

Quest remove your information from our database, please feel free to contact Quest's Privacy Officer at:

Quest Global Research Group Inc.
125 Lakeshore Road East, Suite 305
Oakville, ON L6J 1H3
Canada
E-mail: info@questmindshare.com

You have the right to your information/data you've provided Quest. It is your information. You may request a copy of the information you provide to Quest, and Quest will provide it to you in a timely manner, subject to exceptions under applicable law.



Privacy Policy

[Français](#) / [Deutsch](#) / [Español](#) / [Português](#)

Research For Good Research Participant Privacy Notice

Last Updated: October 3, 2023

Effective Date: October 10, 2023

This Privacy Notice applies to Research for Good Inc ("RFG") and all of RFG's online market research sample sources, including but not limited to SaySo Rewards ("SaySo"), www.SaySoRewards.com. This Privacy Notice defines how RFG collects, stores, uses and discloses your "personal data" or "personal information" or "personally identifiable information" (as defined below). RFG will, and will cause its affiliates to, establish and maintain business procedures that are consistent with this Privacy Notice.

We strive to make our websites, including this Privacy Notice, accessible to individuals with disabilities. If you are having trouble accessing the RFG website or this Privacy Notice,

We use cookies on our website to give you the most relevant experience by remembering your preferences and repeat visits. By clicking "Accept", you consent to the use of ALL the cookies.

[Do not sell my personal information.](#)

[Cookie settings](#) [ACCEPT](#)

WE PROTECT YOUR PRIVACY

RFG is a leading market research company. RFG is strongly committed to protecting the privacy and security of “personal data” or “personal information” or “personally identifiable information” (referred to in this Privacy Notice as “Personal Data”) and conforms its privacy and security practices to applicable laws, and regulations, including, without limitation, the California Consumer Privacy Act (“CCPA”), the California Privacy Rights Act (“CPRA”) and other applicable US State laws, including Virginia, Connecticut Colorado and Utah, the General Data Protection Regulation (“GDPR”) and UK GDPR. . RFG also conforms its privacy and security practices with the codes of standards of applicable market and opinion survey research associations, including, without limitation, ESOMAR (www.esomar.org) and the Insights Association (www.insightsassociation.com).

RFG offers research participants opportunities to take part in market research and express their opinions on a broad range of topics. Our clients and research partners depend on this information to make many decisions that effect the products and services in the global marketplace.

WHAT PERSONAL DATA DO WE COLLECT AND PROCESS?

As used in this Notice, Personal Data means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked with a particular data subject, consumer, or household. Personal Data includes information such as real names, postal addresses, email addresses, and social security numbers.

Personal Data may also include unique identifiers, IP addresses, biometric information, internet or other network activity (such as browsing history, search history, etc.), geolocation data, audio/visual data, and even inferences which may be drawn from any of the above to create a profile about a data subject or consumer.

We may collect Personal Data for the purpose of conducting market research, as expressly stated and agreed to by you, and as otherwise provided in this Privacy Notice. Personal Data collected in connection with market research includes participant names; email addresses; postal addresses; phone numbers; IP addresses; browser fingerprints; device ID; unique identifiers; cookies; geolocation data; web beacons; demographic data, such as age, gender, race/ethnicity, parental status, marital status, postal code, income and education levels; and other information collected through automated means, as described

We use cookies on our website to give you the most relevant experience by remembering your preferences and repeat visits. By clicking “Accept”, you consent to the use of ALL the cookies.

[Do not sell my personal information.](#)

[Cookie settings](#) [ACCEPT](#)

Personal Data may be used and disclosed as described in this Privacy Notice and should not include audio, video, images, or the likeness of anyone other than you.

SENSITIVE INFORMATION

From time-to-time RFG may collect “sensitive personal data” or “sensitive personal information” or “special categories of personal data” (referred to in this Privacy Notice as “Sensitive Personal Data”) which, depending on the country in which you live may include, racial or ethnic origin, health records, financial information, political opinions and religious or philosophical beliefs. If RFG collects your Sensitive Personal Data, RFG will always obtain your explicit consent.

USE OF AUTOMATED DECISION MAKING

If permitted by applicable laws and regulations, we may use automated decision-making to determine the likelihood of fraudulent activity. If our systems determine that your activities associated with you are fraudulent, you may be banned from our services and your profile may be deleted. If you believe that your profile has been wrongfully deleted, please reach us using the contact details in section “Contact Us” at the end of this Privacy Notice.

Automatically collected data may be sent to third-party data processors for the purpose of fraud prevention.

OTHER USES AND SHARING OF INFORMATION

In addition to the uses listed in the table above, we may also use and share your Personal Data:

- in connection with the request or requirement of any lawful request by public authorities;
- to meet national security or law enforcement requirements;
- in connection with the sale, assignment, or other transfer of our business, in which case RFG will make commercially reasonable efforts to ensure that any such buyer agrees to treat Personal Data in accordance with this Privacy Notice;
- if RFG believes that disclosure is necessary or appropriate to prevent physical harm or financial loss or in connection with suspected or actual illegal activity; or
- as otherwise authorized by you.

We use cookies on our website to give you the most relevant experience by remembering your preferences and repeat visits. By clicking “Accept”, you consent to the use of ALL the cookies.

[Do not sell my personal information.](#)

[Cookie settings](#) [ACCEPT](#)

Please note that receiving email communications may be a requirement of your participation in our surveys or research programs. You can opt out from receiving these emails by unsubscribing from the survey or research program.

ADDITIONAL INFORMATION ON INFORMATION COLLECTED THROUGH AUTOMATED MEANS

Cookies

Cookies are small text files stored on your computer by a website that assigns a numerical user ID and stores certain information about your online browsing. We may use cookies on our survey site to help us recognize you as a prior user.

If you wish, you can adjust your web browser's privacy settings to delete cookies upon exiting websites or when you close your browser. You may also configure your browser to block cookies, however doing so may negatively impact your user experience when participating in one of our surveys or other research programs.

Web Beacons

A web beacon (also known as a tag, clear gif or 1×1 pixel), consists of a small string of code that is embedded within a web page or email. There may or may not be a visible graphic image associated with the web beacon, and often the image is designed to blend into the background of a web page or email.

We may use web beacons in our email messages to help determine whether our messages are opened and to verify any clicks through to links within the email. We may use this information to determine which of our emails are more interesting to users, to improve the quality of the emails that we send and to query users who do not open our emails as to whether they wish to continue receiving them. The web beacon is deleted when you delete the email.

If you would prefer not to have web beacons in the emails that you receive, you should adjust your email program to receive messages in plain text rather than HTML. It is also possible to detect and control web beacons that are present on web pages by downloading a plug-in for your browser.

Log Files

We use cookies on our website to give you the most relevant experience by remembering your preferences and repeat visits. By clicking "Accept", you consent to the use of ALL the cookies.

[Do not sell my personal information.](#)

[Cookie settings](#) [ACCEPT](#)

uniquely identify your browser. This information is periodically deleted as part of normal maintenance routines.

Geo-Location Data

RFG may collect geo-location information from your computer or device. RFG may use your geo-location data for fraud prevention or for market research purposes, including but not limited to advertising research or other tracking-based market research activities. RFG will obtain your consent if RFG collects or uses your geo-location information.

Digital Fingerprinting

RFG may use digital fingerprinting technology, also known as “machine identification” technology (“Digital Fingerprinting”), to gather certain data about you and/or your computer.

This data may include Personal Data an Internet Protocol (IP) address, as well as other data such as a computer operating system or browser version number. This technology creates a unique computer identifier (“ID”) that may be used to identify and track your participation in a survey or other research program and limit participation.

RFG may utilize Digital Fingerprinting technology to assist our clients in ensuring the integrity of survey results by enabling us to authenticate users and to help ensure users participate in surveys no more than the maximum allowable participation. In furtherance of RFG’s efforts to assist its clients in protecting and ensuring the integrity of survey results, RFG may: (a) link or associate an ID to an individual or to Personal Data of an individual; (b) share an ID with RFG’s clients and/or sample or panel providers; and/or (c) receive or obtain a unique identifier that is linked to an identified or identifiable individual. Any unique identifier(s) received or obtained by RFG that are linked to an identified or identifiable individual will be protected in accordance with this Privacy Notice.

INFORMATION FOR CALIFORNIA RESIDENTS

The following information applies to residents of California.

Personal Data We Sell or Disclose

CCPA defines the term “sell” broadly. Its meaning includes “renting, releasing, disclosing, disseminating, making available, [and] transferring for monetary or other valuable

We use cookies on our website to give you the most relevant experience by remembering your preferences and repeat visits. By clicking “Accept”, you consent to the use of ALL the cookies.

[Do not sell my personal information.](#)

[Cookie settings](#) [ACCEPT](#)

or certain combinations of anonymized or pseudonymized demographic and other information.

Under the CCPA's definition, we've "sold" the following categories of information to our clients: demographic data, such as age, gender, race/ethnicity, parental status, marital status, postal code, income and education levels.

We've otherwise disclosed the following categories of information, subject to confidentiality restrictions, to our third-party service providers as strictly necessary for them to provide services to us: participant names; email addresses; postal addresses; phone numbers; IP addresses; browser fingerprints; device ID; unique identifiers; cookies; geolocation data; web beacons; demographic data, such as age, gender, race/ethnicity, parental status, marital status, postal code, income and education levels; log files, including Internet Protocol (IP) address, browser type, browser language, the date and time of your request, operating system, referring/exiting pages, and clickstream data; browsing information, such as date and time you visited our website(s), number of pages you viewed, time in seconds you spend on each page, and details of the any website you visited before and/or after participation in one of our surveys or research programs; respondent photos, video, and audio; and social media information (e.g., handles, basic information available on profiles).

When you participate in one of our surveys or research programs, the information you provide or is otherwise collected may be combined with the information of other participants and reported as part of aggregate results. Additionally, the information you provide or is otherwise collected may be used in statistical modeling to better understand trends among the general population. When such statistical modeling is performed, your Personal Data will not be released.

We will not make your Personal Data available to any third party without your consent or required by law, as further specified below.

Notice to California Residents

If you are a California resident, subject to certain exceptions and limitations, you can exercise the rights described below:

- *Your Right to "Know" and to Request Deletion*

We use cookies on our website to give you the most relevant experience by remembering your preferences and repeat visits. By clicking "Accept", you consent to the use of ALL the cookies.
[Do not sell my personal information.](#)

[Cookie settings](#) [ACCEPT](#)

You have the right to request deletion of personal information we've collected or maintain.

To exercise these rights contact us at +1-855-573-2141 or by filling out the form at the following link <https://www.saysorewards.com/ccpa-privacy/>. We may ask you to provide additional information, such as name, email, and participation information in order to verify who is making the request.

Please note that any requested disclosures will only apply to the 12-month period preceding the request, and you are entitled to request disclosure regarding your personal information twice in any 12-month period.

- *Your Right to Opt-Out of the "Sale" of Your Information*

You have the right to opt out of the sale of your personal information. For more information on how to opt out, [please click here](#).

- *Your Right to Non-Discrimination*

You have the right not to receive discriminatory treatment by RFG for the exercise of the privacy rights conferred by the CCPA, including but not limited to by denying you services, charging different prices or rates, or providing you with a different level or quality of services. Please understand, however, that we are in the business of providing market research services to our clients, and any financial incentives we offer to facilitate that goal may be rewarded only if the applicable survey, research project or study is fully and properly completed by the respondent, in the sole discretion of RFG.

- *Your Right to Use an Authorized Agent*

You have the right to designate an authorized agent to make a request under the CCPA on your behalf. To designate an authorized agent, please contact us as provided below. In order to verify you have authorized an agent we will require a signed, written authorization from you.

- *Your Right to Correct Inaccurate Personal Information (Personal Data)*

You have the right to have any inaccuracies about your Personal Data corrected.

- *Your Right to Limit Use and Disclosure of Sensitive Personal Information*

We use cookies on our website to give you the most relevant experience by remembering your preferences and repeat visits. By clicking "Accept", you consent to the use of ALL the cookies.
[Do not sell my personal information.](#)

[Cookie settings](#) [ACCEPT](#)

This information may include: your full name, birth date, phone number, email address, or other basic personal information about you that we already have on file.

- *Notice of Financial Incentive*

RFG may offer opportunities for you to earn money and rewards by completing survey or research programs. Participation in these offerings may require you to provide Personal Data.

For more information about how to opt into these offerings, or about how to opt out once you have opted in, see the notices and official rules accompanying these incentives.

If you have any questions or want to exercise any of these rights, you may contact us with such a request please contact us at **privacy@researchforgood.com** or via mail at:

Research for Good

1037 NE 65th St #80212

Seattle, WA 98115

VIRGINIA, CONNECTICUT, COLORADO AND UTAH RESIDENTS

The following information applies to residents of Virginia, Connecticut, Colorado and Utah.

If you are a resident of Virginia, Connecticut, Colorado or Utah, pursuant to your applicable state's privacy laws and regulations and subject to certain exceptions and limitations, you can exercise the rights described below:

- *Your Right to Access Your Personal Data*

You have the right to access your Personal Data.

- *Your Right to Obtain a Copy of Your Personal Data*

You have a right to obtain a copy of your Personal Data in a portable and, to the extent technically feasible, a readily usable format.

- *Your Right to Have Your Personal Data Deleted*

We use cookies on our website to give you the most relevant experience by remembering your preferences and repeat visits. By clicking "Accept", you consent to the use of ALL the cookies.

[Do not sell my personal information.](#)

[Cookie settings](#) [ACCEPT](#)

- *Your Right to Opt-Out of the Processing of Your Personal Data*

You have the right to to opt out of the processing of your Personal Data for specific purposes subject to the applicable law and regulation in your state.

If you have any questions or want to exercise any of these rights, you may contact us with such a request please contact us at **privacy@researchforgood.com** or via mail at:

Research for Good

1037 NE 65th St #80212

Seattle, WA 98115

INFORMATION FOR CITIZENS OF THE EU, UK AND SWITZERLAND

Cross-Border Transfers

Research for Good complies with the EU-U.S. Data Privacy Framework (EU-U.S. DPF), the UK Extension to the EU-U.S. DPF, and adheres to the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) as set forth by the U.S. Department of Commerce. Research for Good has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) with regard to the processing of Personal Data received from the European Union in reliance on the EU-U.S. DPF and from the United Kingdom (and Gibraltar) in reliance on the UK Extension to the EU-U.S. DPF.

Research for Good has certified to the U.S. Department of Commerce that it adheres to the Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) with regard to the processing of Personal Data received from Switzerland in reliance on the Swiss-U.S. DPF. If there is any conflict between the terms in this privacy notice and the EU-U.S. DPF Principles and/or the Swiss-U.S. DPF Principles, the EU-U.S. DPF Principles and/or the Swiss-U.S. DPF Principles shall govern. To learn more about the Data Privacy Framework (DPF) program, and to view our certification, please visit <https://www.dataprivacyframework.gov/>.

With respect to Personal Data received or transferred pursuant to the EU-U.S. DPF, the UK extension to the EU-US DPF and the Swiss-U.S. DPF, RFG is subject to the regulatory enforcement powers of the U.S. Federal Trade Commission.

Pursuant to the EU-U.S. DPF Principles and/or the Swiss-U.S. DPF Principles, EU, UK and Swiss individuals have the right to obtain our confirmation of whether we maintain

We use cookies on our website to give you the most relevant experience by remembering your preferences and repeat visits. By clicking "Accept", you consent to the use of ALL the cookies.

[Do not sell my personal information.](#)

[Cookie settings](#) [ACCEPT](#)

their query to privacy@researchforgood.com. If requested to remove data, we will respond within a reasonable timeframe.

We will provide an individual opt-out choice (for Personal Data) or opt-in choice (for sensitive data) before we share your data with third parties other than our agents, or before we use it for a purpose other than which it was originally collected or subsequently authorized. To request to limit the use and disclosure of your Personal Data, please submit a written request to privacy@researchforgood.com.

RFG's accountability for Personal Data that it receives in the United States under the EU-U.S. DPF Principles and/or the Swiss-U.S. DPF Principles and subsequently transfers to a third party is described in the EU-U.S. DPF Principles and/or the Swiss-U.S. DPF Principles. In particular, RFG remains responsible and liable under the EU-U.S. DPF Principles and/or the Swiss-U.S. DPF Principles if third-party agents that it engages to process the Personal Data on its behalf do so in a manner inconsistent with the EU-U.S. DPF Principles and/or the Swiss-U.S. DPF Principles, unless RFG proves that it is not responsible for the event giving rise to the damage.

In compliance with the DPF Principles, RFG commits to resolve complaints about your privacy and our collection or use of your Personal Data transferred to the United States pursuant to the Data Privacy Framework. European Union, United Kingdom, and Swiss individuals with DPF inquiries or complaints should first contact RFG at:

Privacy Compliance Officer

Research for Good

1037 NE 65th St #80212

Seattle, WA 98115

In compliance with the EU-U.S. Data Privacy Framework (EU-U.S. DPF), the UK Extension to the EU-U.S. DPF, and adherence to the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), Research for Good commits to resolve complaints about our collection or use of your personal information transferred to the U.S. pursuant to the EU-U.S. DPF, the UK extension to the EU-U.S. DPF, and the Swiss-U.S. DPF. EU, UK, and Swiss individuals with inquiries or complaints should first contact Research for Good.

We use cookies on our website to give you the most relevant experience by remembering your preferences and repeat visits. By clicking "Accept", you consent to the use of ALL the cookies.

[Do not sell my personal information.](#)

[Cookie settings](#) [ACCEPT](#)

If your DPF complaint cannot be resolved through the above channels, under certain conditions, you may invoke binding arbitration for some residual claims not resolved by other redress mechanisms. See <https://www.dataprivacyframework.gov/s/article/ANNEX-I-introduction-dpf>

Notice to EU, UK (and Gibraltar) and Swiss Residents

You have the right to review, correct, or delete your Personal Data. Specifically:

- *Right of access*

You have the right to obtain confirmation and information about the processing of your Personal Data.

- *Right to rectification*

You have the right to have any inaccuracies about your Personal Data corrected.

- *Right to erasure*

You have the right to have your Personal Data deleted (this right is limited to data which according to law and regulation may only be processed with your consent, if you withdraw your consent for processing)

- *Right to restriction of data processing*

You have the right to require that the processing of your Personal Data be restricted (during the course of any investigation into honoring your request, RFG's access your Personal Data will be limited)

- *Right to data portability*

You have the right to have your Personal Data transferred to another party (this right is limited to data provided by you)

If you have any questions or want to exercise any of these rights, you may contact us with such a request please contact us at privacy@researchforgood.com or via mail at:

Research for Good

We use cookies on our website to give you the most relevant experience by remembering your preferences and repeat visits. By clicking "Accept", you consent to the use of ALL the cookies.
[Do not sell my personal information.](#)

[Cookie settings](#) [ACCEPT](#)

privacy and our collection or use of your Personal Data these citizens or residents can address inquiries or complaints regarding this Privacy Notice should contact RFG at privacy@researchforgood.com.

DO WE COLLECT INFORMATION FROM CHILDREN?

RFG does not knowingly collect Personal Data from children below 16. If RFG becomes aware that RFG has inadvertently collected Personal Data from a child below the age where parental consent is required, RFG will delete such Personal Data from our database.

WHAT SAFEGUARDS HAVE WE IMPLEMENTED TO HELP ENSURE THE SECURITY OF YOUR PERSONAL INFORMATION?

The security of your Personal Data is very important to us. We have put in place reasonable physical, electronic, and administrative procedures to safeguard the information we collect.

Only those employees who need access to your information in order to perform their duties are authorized to have access to your Personal Data.

We cannot guarantee that all communications between us or information stored on our servers will be free from unauthorized access by third parties such as hackers, and your use of our services demonstrates your assumption of this risk.

HOW DO I OPT-OUT OF SURVEYS OR OTHER RESEARCH PROGRAMS?

Your decision to participate in a survey or other research program, respond to any specific survey question or provide Personal Data or Sensitive Personal Data, will always be respected.

You may choose whether or not to participate in a particular survey or research program or discontinue participation at any time. However, failure to provide certain information or fully participate in a particular survey may preclude you from receiving incentive compensation or participation in future certain research studies.

If you decide not to participate in a survey or other research program, you can click the unsubscribe hyperlink within the e-mail and you will no longer receive survey or other research program invitations. You can also e-mail us at privacy@researchforgood.com.

We use cookies on our website to give you the most relevant experience by remembering your preferences and repeat visits. By clicking "Accept", you consent to the use of ALL the cookies.

[Do not sell my personal information.](#)

[Cookie settings](#) [ACCEPT](#)

carefully read the privacy notices or policies of each site that you visit for information on their privacy, security, data collection and distribution policies.

CLASS ACTION WAIVER

Any arbitration or court trial, related to any claim under this Privacy Notice, whether before a judge or jury or pursuant to judicial reference, will take place on an individual basis, without resort to any form of class or representative action ("Class Action Waiver"). THIS CLASS ACTION WAIVER PRECLUDES ANY PARTY FROM PARTICIPATING IN OR BEING REPRESENTED IN ANY CLASS OR REPRESENTATIVE ACTION REGARDING A CLAIM UNDER THIS NOTICE. Regardless of anything else herein, the validity and effect of the Class Action Waiver may be determined only by a court and not by an arbitrator. THIS CLASS ACTION WAIVER IS VOID WHERE LIMITED OR PROHIBITED BY LAW.

CONTACT US

We value your opinion. If you have questions, comments or suggestions, or if you would like to opt-out of our surveys or other research programs, please contact us at **privacy@researchforgood.com** or via mail at:

Research for Good

1037 NE 65th St #80212

Seattle, WA 98115

Attn: Privacy Compliance Officer

Need more info? Send us a message, we love hearing from you.

Say Hi

We use cookies on our website to give you the most relevant experience by remembering your preferences and repeat visits. By clicking "Accept", you consent to the use of ALL the cookies.

[Do not sell my personal information.](#)

[Cookie settings](#) [ACCEPT](#)

What personally identifiable information does Torfac collect from me?

Torfac collects information in several ways from different parts of our website and network. Some information is gathered when you sign up. During member registration, **Torfac** asks for your name, email address, zip code and household information. The more information you volunteer to provide accurately, the better we are able to offer you services and rewards. Additionally, if you ever contact **Torfac** through any means, we may keep a record of that correspondence. Whenever **Torfac** collects any such information, we aim to include a link to this Privacy Policy on that page.

What are cookies and how does Torfac use them?

A cookie is a packet of electronic data sent to your browser, from a web server and stored on your computer's hard drive. As part of offering your specific surveys, information, and personalized services, **Torfac** may use cookies to store and sometimes track information about you. **Torfac** may require that you accept cookies for preparing such specific content for you. This also avoids you having to enter your login information every time.

Who is collecting information and for what purpose?

Torfac collects several information through surveys and registration and other means, which helps its research clients develop new products and services for consumers. You are sharing that information with **Torfac** only, unless it is specifically stated otherwise on any survey you participate in. If data is being collected and/or maintained by any company other than **Torfac** sites, you will be notified prior to the time of the data collection or transfer. If you do not want your data to be shared, you may choose not to allow the transfer by not using that particular survey or product.

Rewards and promotions that we offer on **Torfac** may be either sponsored by other companies independently, or may be co-sponsored by **Torfac** and another company. Some data collected during such a promotion may be shared with the sponsor. However, you will be notified prior to the time of data collection or transfer. You can decide not to participate in that particular promotion if you do not want to share your data.

Any specific Sensitive Information (like information specifying medical or health conditions, racial or ethnic origin, political views, religious or spiritual beliefs, trades and union membership or information specifying the sex life of the individual) will be treated with additional care. If **Torfac** intends to share such information to another company for a different purpose than originally collected, then you will be expressly asked permission prior to any such disclosure.

With whom does Torfac share my information?

We take privacy very seriously. **Torfac** will not disclose any of your personally identifiable information except when we have your explicit permission or under any special

circumstances that the law requires it or under the circumstances specified in detail below. The following describes some of the ways that your information may be disclosed.

Please see the Terms of Service for our services for more detailed information about how your personal information may be shared.

Business Partners, Clients & Sponsors:

Torfac may disclose your personal information to our partners, clients or sponsors. However, if any personal data about you were ever to be shared, we will tell you before we collect or transfer the data. Many activities we offer request additional information from sponsors. By requesting more information, you give **Torfac** permission to share your information with the sponsor so they can fulfil your request. In many instances, only your email address will be shared. If more information will be shared with our partners, you will be notified in advance. From time to time, you may be offered the opportunity to receive test materials, or other products or special offers from our partners. If you opt-in to receive information from these third parties, **Torfac** will (with your permission) share your name and email address with them.

Torfac may also disclose personal information in some special cases when disclosing this information is necessary to identify, contact or bring legal action against someone who may be violating **Torfac's** policies and Terms of Service or may be causing any injury to or interference with (either intentionally or unintentionally) **Torfac's** products, services, rights or property, other **Torfac** members and users, or anyone else that could be affected by any such activities. **Torfac** may disclose or access account information when we believe in good faith that the law requires it and for administrative and other purposes that we deem necessary to maintain, service, and improve our products and services.

What are the legal bases we use for processing your information?

Torfac is committed to Privacy and Data protection. Our privacy policy adopts the principles of General Data Protection Regulation issued by the European Union ("GDPR") as a benchmark to which we, our employees and suppliers adhere.

What are my choices regarding collection, use, and distribution of my information?

Only **Torfac** (or partners working with **Torfac** under confidentiality agreements) will send you any direct mails, only if you indicate that you do not object to these. You also have choices with respect to how cookies work. By changing your internet browser settings, you have the choice to accept all cookies, notified when a cookie is set, or to reject all cookies requested. If you choose to reject all cookies, you will be unable to use those **Torfac** services that do require prior registration in order to participate. **Torfac** does not sell or lease any user information to anyone. We will always notify you at the time of data collection or transfer if your data will be shared with any third party and you will always have the option of not allowing it to be shared.

What else should I know about my privacy?

Please keep in mind that whenever (and wherever) you choose to disclose personal information online – for example through emails, social networking websites, blogs, or in chat areas that information can be collected and used by any other user. If you post personal information online that is accessible to the public, you may receive unsolicited messages from other parties in return. Ultimately, you are solely responsible for maintaining the secrecy of your passwords and/or any account information. Please be careful and responsible whenever you're online.

How does Torfac protect the privacy of my children?

Torfac obtains prior parental consent where surveys require children to participate and parental supervision is also required for any such surveys with children ages 6-15. We take special extra care to protect the safety and privacy of young users on our site, and we encourage you to participate in your child's experience online. We do not permit any marketing or in children's research and the certain topics are completely prohibited in research among children: Name/account name/E-mail or physical address, Phone number, Race or Ethnicity, Religion or Cast, Household income, Family illness, Marital status. of parents or other family members, Relationship matters, Grades in school or college, Alcohol, Sexual Issues, Tobacco and Firearms.

Special Note to International Users

The Site is hosted in the United States. If you are a User accessing the Site from the European Union, Asia, or any other region with laws or regulations governing personal data collection, use, and disclosure, that differ from United States laws, please note that you are transferring your personal data to the United States which does not have the same data protection laws as the EU and other regions, and by providing your personal data you consent to:

The use of your personal data for the uses identified above in accordance with the Privacy Policy; and the transfer of your personal data to the United States as indicated above. YOU ACKNOWLEDGE THAT THE LAWS OF THE UNITED STATES TREAT YOUR INFORMATION IN A MANNER THAT MAY BE SUBSTANTIALLY DIFFERENT FROM, AND LESS PROTECTIVE THAN, THE TREATMENT REQUIRED UNDER THE LAWS OF OTHER COUNTRIES AND JURISDICTIONS. IF YOU DO NOT WANT YOUR INFORMATION TRANSFERRED TO THE UNITED STATES, YOU SHOULD NOT SHARE YOUR INFORMATION WITH US, OR MAKE USE OF THE SITE.

TO THE EXTENT ALLOWED BY THE LAW OF THE COUNTRY IN WHICH YOU ARE LOCATED, YOU EXPRESSLY WAIVE ANY RIGHT YOU MAY HAVE TO REQUIRE US TO TREAT YOUR IDENTIFYING INFORMATION IN ACCORDANCE WITH THE LAWS OF ANY COUNTRY OR JURISDICTION OTHER THAN THE UNITED STATES. HOWEVER, THE FOREGOING WAIVER MAY NOT BE LEGALLY BINDING IN SOME COUNTRIES, SUCH AS THE MEMBER STATES OF THE EUROPEAN UNION. TO THE EXTENT IT IS NOT LEGALLY BINDING IN THE COUNTRY IN WHICH YOU ARE LOCATED, THIS FOREGOING WAIVER DOES NOT APPLY TO YOU.

Changes and Updates to this Privacy Policy

Torfac reserves the right, at our discretion, to change, modify, add, or remove portions of this Privacy Policy at any time for any reason. Each time **Torfac** exercises such a right, you shall be required to affirmatively accept the updated Privacy Policy, and if you fail to do so, you will no longer be able to access or use the Site.

Additional Information

Any other questions regarding this should be sent to letstalk@torfac.com

Privacy Policy

Summary

BEFORE USING OUR SERVICES, PLEASE READ THE ENTIRE TERMS OF SERVICE BELOW. THIS SUMMARY ONLY INCLUDES SOME KEY POINTS REGARDING YOUR MEMBERSHIP.

Sampoolish is only for your personal, noncommercial use. By participating as a panelist, you agree to deal fairly and professionally with us and with other Sampoolish members. While you control how often you participate, our clients control administration of their own surveys. Points may be accrued at varying rates but can only be redeemed in 25,000-point (\$25 equivalent) increments. The Sampoolish system only works properly if our members answer surveys thoughtfully and truthfully, and do not try to “game the system” by speeding through surveys, providing meaningless answers, or otherwise taking surveys in bad faith. We reserve the right to deactivate a member’s account for any reason.

Welcome to the Sampoolish website (the “Site”), owned and operated by Solugo (referred to herein as “Sampoolish”). By accessing, browsing, or using the Site or other services described below, you acknowledge you have read, understood, and agreed to be bound by these Terms of Service (“Terms”). These Terms govern your use of Sampoolish’s services, including but not limited to: (1) use of the Site; (2) registration as a member (“Member”); (3) participation on a panel; (4) use of any mobile applications operated by Sampoolish (also included as part of the “Site”); and (5) participation in any survey or study offered, provided, hosted, or administered by or through Sampoolish (collectively, and inclusive of items 1 through 5, the “Service(s)”). If you do not agree to these Terms, you should not access the Services. Sampoolish reserves the right to refuse, restrict, prohibit, or reject your access to the Services, at any time, for any reason. Our collection and use of your personal information is also governed by our Privacy Policy, and our administration of sweepstakes is governed by the Sampoolish DailySweeps Official Rules, each of which are incorporated into these Terms by this reference. Sampoolish reserves the right to revise these Terms at any time by updating this posting. You are encouraged to review these Terms each time you use the Services because your use of the Services after the posting of changes will constitute your acceptance of the changes.

1. We protect your privacy

SurveyExchange is committed to respecting individual and client privacy, to safeguarding confidential information and to ensuring the security of all personal information. When you decide to share your information with us, we feel it is important to assure you your information will be safely protected. This statement discloses our information collecting, handling, and disclosure practices.

2. what do we do?

SurveyExchange is an online panel company focused on providing quality survey responses to our clients which represent the Market Research industry. SurveyExchange is headquartered in Faridabad, Haryana with offices around India.

3. Personal Information

We collect personal information from you when you communicate with us by any media. The personal information collected on this website may be e.g., your name, company, title, phone number, email address, or other information you provide. The collection of personal information is voluntary. Other than as set forth in this Privacy Policy, SurveyExchange will not disclose any of your personally identifiable information except when we have your permission or under special circumstances, such as when we believe in good faith the law requires it or under certain circumstances. The following describes some of the ways your information may be disclosed.

4. Business Partners & Sponsors

Subject to the other applicable provisions herein, SurveyExchange may disclose your personal information to business partners or sponsors. Our members are occasionally presented opportunities to request additional information from sponsors about said sponsors promotions. By requesting more information on the opportunities, you give SurveyExchange permission to transfer your personal information to the sponsor so they can fulfil your request. In many instances, only your email address will be shared.

5. Third Party Data & Data in the Aggregate

Under confidentiality agreements, SurveyExchange may match user information with third party data. Also, SurveyExchange discloses aggregated user statistics in order to describe our services to prospective partners, advertisers, and other third parties, and for other lawful purposes. SurveyExchange may also disclose account information in special cases when we have reason to believe disclosing this information is necessary to identify, contact, or bring legal action against someone who may be violating SurveyExchange Terms & Conditions or may be causing injury to or interference with (either intentionally or unintentionally) SurveyExchange rights or property, other SurveyExchange users, or anyone else who could be harmed by such activities.

Finally, if there is a sale of a majority of the shares or assets of the legal entities owning and operating SurveyExchange, you agree your personal information and data may be transferred or assigned to such new owners.

6. Opt Out

We may use your personal information ourselves to conduct direct marketing when you have opted into this, but you are entitled to opt out from receiving direct marketing communications from us at any time. You may do so by responding to the opt out option which is included with each direct marketing communication we send.

7. European Economic Area (“EEA”)

Please note: information displayed on our Website or sent to SurveyExchange over the Internet may be transferred outside of the EEA, if you have given your consent. data will only be sent to other offices within SurveyExchange in the case you require:

- more information on SurveyExchange;
- a quote request; or
- anything else pertaining specifically to SurveyExchange.

If you have any concerns in relation to such transfers, you should not use the Internet as a means of communication with SurveyExchange.

8. How we protect your personal information

SurveyExchange takes reasonable steps to protect your personal information from unauthorized access, use, disclosure, or loss. This site has security measures (including online and offline physical, electronic, and managerial safeguards) in place to protect against the loss, misuse, and alteration of the information, including your e-mail address, under our control.

We recommend you do not divulge your password to anyone. SurveyExchange will never ask you for your password in an unsolicited phone call or in an unsolicited email. Also remember to sign out of your SurveyExchange account and close your browser window when you have finished your work. This is to ensure others cannot access your personal information and correspondence if you share a computer with someone else or are using a computer in a public place like a library or Internet cafe.

Unfortunately, no data transmission over the Internet can be guaranteed to be 100% secure. As a result, while we strive to protect your personal information, SurveyExchange cannot ensure or warrant the security of any information you transmit to us or from our online products or services, and you do so at your own risk. Once we receive your transmission, we make our best effort to ensure its security on our systems.

9. Disclosure of your personal information

We do not share, sell, rent, or trade personally identifiable information with third parties; however to assist us in the delivery of our service offerings we may share your personal information with third party suppliers such as those who provide and manage incentives in connection with the completion of surveys, data hosting and storage services, third party technology providers, data matching providers to facilitate analytic and related objectives, and other consultants who we retain from time to time. These third parties are bound by confidentiality obligations and will not use your information for purposes outside of those specified herein. We also reserve the right to disclose your personally identifiable information as required by law or when we believe the disclosure is necessary to protect our rights and/or comply with a judicial proceeding, court order, national security requirement, or legal process served on our website.

10. Use of Cookies

A cookie is a small amount of data sent to your browser from a web server and stored on your computer's hard drive. We may use technology to track the patterns of behavior of visitors to the site. Currently, cookies are utilized by SurveyExchange within the following four primary categories or uses:

1. business cookies which operate as a quality control and verification mechanism in connection with the survey process;
2. performance cookies so traffic patterns and uses on the SurveyExchange website may be measured and optimized;

3. user cookies so user information may be recorded so as to enhance performance and user experience on the website; and
4. targeting cookies which are utilized to measure web viewing for market research purposes.

Tracking cooking will help us to speed up your future activities at the site and allow SurveyExchange to provide you with information specifically tailored to your interests. You can usually modify your browser to prevent this happening.

The information collected in this way can be used to identify you unless you modify your browser settings. To modify your browser settings, click on the help section of your Internet browser and follow the instructions. Please note: not accepting cookies may affect the performance of our website.

From time to time, SurveyExchange collaborates with third parties (including clients) to enable the use of targeting cookies, web beacons, pixels, SDK's, and mobile device identifiers to measure web-viewing and mobile use activities, for behavioral measurement purposes, in connection with ad exposure and display advertising for market research purposes and other related activities. You also agree web beacons and pixels may appear and/or be activated to collect information from emails you open. To facilitate these services, SurveyExchange's clients (or their agents) or other collaboration partners may write, set, or read:

- cookies,
- locally shared/stored objects,
- flash cookies and
- other related technologies ("Third Party Technologies").

If you participate, your Member ID will be stored in, or associated with, Third Party Technologies to allow you to be contacted about online ads, promotions, or in connection with market research surveys. SurveyExchange's clients (or their agents) will use the Third Party Technologies to determine whether you have seen, clicked on, or otherwise interacted with the online ad or promotion. SurveyExchange will share your Member ID name, postal address, email address, or Device ID with SurveyExchangeclients (or their agents) so you will have an opportunity to receive a promotion, be contacted about an online ad, complete a survey, or so data previously collected by SurveyExchange, such as age, gender, income, etc. ("Audience Measurement Data") may be shared with third parties, including without limitation SurveyExchange's subcontractors, partners, and/or clients for the purpose of audience measurement reporting on the advertising, advertising or other promotional campaigns, and websites you visit, view, and/or click on. The Audience Measurement Data will be used to assist in the creation, development, and implementation of websites, online advertisements, and other Internet and digital media features, functionality, and campaigns. Your data may be transferred outside of the country from which it was originally collected. To learn more about interest-based advertising in general and to opt out, please visit www.aboutads.info/choices.

11. Children's Privacy

SurveyExchange encourages all parents and guardians to instruct their children in the safe and responsible use of their personal information whilst using the Internet. SurveyExchange will not (through our website or otherwise) intentionally collect information relating to or originating from a child unless we have the consent of the child's parent or guardian. If we become aware a user of our website is a child who is using this website without the consent of his parent or guardian, we will use reasonable endeavours to delete any information submitted by that child as soon as possible and to ensure such information is neither transferred to anyone else nor used by us. Please let us know as soon as you become aware a child has submitted information about him/herself through our website without the consent of his parent or guardian. You can contact us in the ways outlined at the end of this policy.

12. Check for changes to our Privacy Statement

Please check this page periodically for changes as SurveyExchange reserves the right, at its discretion, to change, modify, add, or remove portions of the Privacy Policy and the Site at any time. Your continued use of the Site following the posting of any changes to this Policy will mean you accept such changes. If we are going to use personal data in a manner materially different from as stated at the time of collection, we will notify the affected individuals by posting a notice on this Site or via email.

13. Governing Law

This Site and Privacy Policy are governed by the laws of India. Any dispute arising in connection with this Privacy Policy shall be governed under the jurisdiction of the courts of India.

14. How to contact us and unsubscribe your email

Questions regarding this policy, complaints about our practices and access requests should be directed to the SurveyExchange Team via e-mail: support@SurveyExchange.com To unsubscribe your email account and not receive any further emails from SurveyExchange, please send an email (from the address used as your SurveyExchange member contact) to support@SurveyExchange.com with "unsubscribe" as the subject line

15. Termination

You agree to

- a. provide accurate, current, and complete information about you as may be prompted by any registration forms on the Services;
- b. maintain the security of your password and login credentials; and
- c. maintain and promptly update the information you provide during registration, and any other information you provide to SurveyExchange, so as to keep it accurate, current, and complete.

Registration requires information includes, without limitation, your full legal name, gender, primary language, your date of birth, the country and state/province of your primary residence, your phone number, and your current working email address. Your failure to provide accurate information, or if SurveyExchange determines fraudulent information was provided by you in connection with your registration and/or you otherwise engaged in any other inappropriate activity (as determined by SurveyExchange in its sole discretion), SurveyExchange may cancel or invalidate your account(s), registrations, and Rewards, deny redemption of your Rewards, or restrict, block, limit, and prevent your access to and use of the Services and, further, all Rewards, incentives and other consideration shall be subject to forfeiture. All points earned will be expired automatically upon 12 months of inactivity.

16. Non-Use and Nondisclosure

Information and content made available to you in the Services may contain trade secrets or other confidential or proprietary information of SurveyExchange and/or SurveyExchange's clients, suppliers or licensors. You must hold in strict confidence, and not disclose to any other person, any information and content you access or learn in connection with your participation in any survey, project, questionnaire, or other market research-related activity related to the Services. You are prohibited from sharing with any third party, photographic or other imagery, information, or any other content from any and all activities within or from the Site. You must not use any such information or content for any purpose other than your participation in the Services in accordance with this Agreement. You hereby agree to notify SurveyExchange immediately if you learn of or suspect any use or disclosure of, or access to, any such information or content other than as specifically authorized in this Agreement.

17. EU-IN and Swiss-IN Privacy Shield

Although we are not yet Privacy Shield certified, SurveyExchange adheres to the Privacy Shield Principles of Notice, Choice, Accountability for Onward Transfer, Security, Data Integrity and Purpose Limitation, Access, and Recourse, Enforcement and Liability. If there is any conflict between the policies in this privacy policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern.

18. Complaints

In compliance with the EU-US and Swiss-US Privacy Shield Principles, SurveyExchange commits to resolve complaints about your privacy and our collection or use of your personal information. European Union individuals with inquiries or complaints regarding this privacy policy should first contact SurveyExchange at:

SurveyExchange

Attn: Privacy Policy Support

238-239, 2nd Floor, SRS IT Tower, Mathura Road

Faridabad, HR 121001

Email: support@SurveyExchange.com

© 2023 Surveyexchange | All Rights Reserved

[Privacy Policy](#)

[Terms and Conditions](#)

Follow us  

Privacy policy

Last reviewed: March 2024

1 Purpose of this privacy notice

At Savanta we provide various market research services including designing market research surveys, hosting opinion panels and providing audience research services and statistical analytics to global businesses ("**Services**"). We are committed to protecting the privacy of our website visitors, clients and, as a market research group, the privacy of research respondents in connection with the provision of our Services. We want to provide a safe and secure service where we deal with your personal data.

This Privacy Notice sets out how processes your personal data in connection with the provision of our Services (including our services offered through our Vue Product Range) and our websites at and <https://opinionpanel.co.uk> ("**Sites**"). This Privacy Notice also sets out your rights in respect of our processing of your personal .

When we talk about "personal data", we mean any information which relates to an identified or identifiable living individual. Individuals might be identified by reference to a name, an identification number, location data, an online identifier (such as an IP address) or to other factors that are specific to them, such as their physical appearance.

This Privacy Notice is intended to assist you in making informed decisions when using our Sites and our Services. Please take a moment to read and understand it. It should be read in conjunction with our .

Please note your access to and use of our Sites and/or Vue Product Range including your -Vue account page and any secure area, is subject at all times to separate Terms of Use and/or Terms of Service.

2 Changes to this Privacy Notice

We will update this Privacy Notice from time-to-time to reflect any changes or proposed changes to our use of your personal data, or to comply with changes in applicable law or regulatory requirements. We may notify you by email of any significant changes to this Privacy Notice, but we encourage you to review this Privacy Notice periodically to keep up to date on how we use your personal data.

3 About Us

The Sites and our Services are made available by various companies in the Savanta group of companies (each a “**Group**”).

Where this Privacy Notice refers to “**Savanta**”, “**we**”, “**us**”, “**our**”, this means Savanta Group Limited, or one or more of the particular Group Companies that provide the particular Site or Services to you.

We set out below more information about our Group Companies, including their location and respective roles and responsibilities.

-

Location: United Kingdom

Savanta Group Limited (company no: SC 281 352) is a company established under the laws of Scotland with its registered office at C/O Bellwether Green Limited, 225 W George St, Glasgow G2 2ND.

Location: USA

Savanta Group LLC (company no: 200823810071 is a company established under the laws of the United States with its registered office at 300 California Street, Suite 200, San Francisco, CA 94104.

Location: Canada

Savanta Analytics Ltd (BN 749932919, Registry ID BC1167318, registered in Vancouver, CA)

Location: India



Savanta Analytics Private Limited (CIN U74999UP2020PTC133576, PAN ABECS3099M, TAN MRTS20085C)

Except as stated otherwise, each Group Company is an independent controller of your personal data. However, in connection with the provision of our Services, we may carry out certain activities referred to in this Privacy Notice in our capacity as a data processor acting on behalf of our clients. We have made this distinction clear in the Privacy Notice.

4 How to contact us

If you have any questions about this Privacy Notice or want to exercise [your rights as a data subject](#) set out in this Privacy Notice, you can contact us using the following methods:

On Site	Contact us using our Enquiry Form.
Email	Send us an email at: dpo@savanta.com .
Post	Write to us at: Savanta DPO, 60 Great Portland Street, London, W1W 7RT.
Telephone	Call us on: +44 (0)20 7632 3434 (UK EMEA) or +1 (917) 768-2710 (Canada).

5 What personal data we collect

In providing our Sites and Services, we may collect and process different types of personal data about you for different processing purposes. The types of personal data we collect depends on who you are and how you use our Site and Services and includes the following:

Identity Data	First name; last name.
Contact Data	Home address; billing and/or delivery address; email address; telephone number.
Respondent Data	Account username; password; first name; last name; date of birth; gender; country; nationality; username; job title; social status; sexual orientation; whether you have participated in any survey or questionnaire responses and feedback; survey responses, participation in any promotions or competitions.
Image Data	Photos; video recordings.
Financial Data	Bank account details; partial payment card details and details about payments made between you and us.
Behavioural Data	Data relating to your browsing activity or interaction with our emails, obtained through the use of cookies, pixel tags and other similar technologies; information

	about when your current or previous sessions started; details about any products you viewed or purchased through the Sites.
Technical Data	IP address; browser type and operating system; geolocation, to ensure we're showing you the correct notices and information; any other unique numbers assigned to a device.
Job Applicant Data	Date of birth; gender; country; nationality; CVs; work experience; dietary requirements; any other personal data you may provide in advance of/during your supply of services to us.
Marketing and Communications Data	Marketing preferences; service communication preferences.
Publicly Available Data	Information about articles (or similar) that you may have published; information about your interests or affiliations or publicly stated positions on political matters, corporate matters and similar.

6 How we collect and receive personal data

We collect and receive personal data using different methods:

Personal data you provide to us	You may give us your personal data directly, for example, when you agree to take part in market research opinion panels, or when you provide your Contact Data as part of a survey, purchase services via our Site, contact us with enquiries, complete forms on our Site, subscribe to receive our marketing communications or provide feedback to us.
Personal data we collect using cookies and other similar technologies	When you access and use our Site, we will collect certain Behavioural Data and Technical Data. We collect this personal data by using cookies and other similar technologies (see the "Insight, analysis and retargeting through Cookies" section below).
Personal data received from third parties	We may receive personal data about you from third parties. Such third parties may include our clients, market research sample and list suppliers, analytics providers, data brokers and third party directories.
Publicly available personal data	From time to time, we may collect personal data about you (Identity Data and Contact Data) that is contained in publicly available sources (including open source data sets or media reports) or that you or a third party may otherwise make publicly available (for example through speeches at events or publishing articles or other news stories or posts on social media platforms).

7 Who we collect personal data about

We collect and process personal data from the following people:

Site visitors	If you browse our Site or register an account on our Site, we will collect and process your personal data in connection with your interaction with us and our Site.
People who contact us with enquiries	If you contact us with an enquiry through our Site, submit a complaint through our Site or provide any feedback, we will collect and process your personal data in connection with your interaction with us and our Site.
Respondents	If you participate in one of our surveys or panels, we will process your data including Respondent Data and Financial Data in connection with your participation.
People who work for our clients and suppliers	If you work for one of our clients or suppliers and have responsibility for placing orders with us, administering your organisation's account with us or handling our orders or our account with your organisation, we will process your personal data in connection with your organisation's relationship with us.
Talent	If you supply services and/or content to us and work with us to provide services to our client (including feature in content we produce), we may collect and process your personal data, such as your Identity Data, Contact Data, Financial Data, CVs in connection with such supply of services and/or content to us and our clients.
Partner/supplier personnel	If you (or your organisation) supply products or services to us or otherwise partner with us, we may collect and process your personal data in connection with our receipt of those products and services and/or partnership. This may include personal data included in any email or telephone communications or recorded on any document relating to an order for the products or services, such as your Contact Data.
Visitors to our physical locations	If you attend one of our offices or other locations, we may process personal data that you volunteer in connection with your visit and any enquiries you make. For example, you may volunteer personal data when asking us to assist you in finding accommodation or transportation suitable for your needs, or when signing in as a guest. CCTV footage may also be collected for security purposes.
Event attendees	If you attend one of our events, we will process personal data about you in connection with your attendance at the event. For example, we may ask you to complete a registration or feedback form, or other document relating to the event.
Job applicants	If you apply for a job with us, whether through the Site or otherwise, we will collect and process your personal data in connection with your application.

Members of the public

We may collect and process your data that you volunteer or where you have indicated to us, market research sample or list providers that you are willing to take part in market research and/or opinion panels in connection with the provision of Services to our clients.

8 How we use your personal data

We use your personal data for the purposes set out in this section. If we wish to make any changes to these purposes, or if we wish to use your personal data for any purpose that is not listed in this section, we will notify you using the contact details we hold for you.

A: Use of our Sites

When you browse our Sites, we collect and process Behavioural Data and Technical Data to help us understand how you are using and navigating our Sites. We do this so that we can better understand which parts of our Sites are more or less popular and improve the structure and navigation of our Sites.

Our legal basis for processing**If you browse our Sites**

It is in our legitimate interest to use personal data in such a way to ensure that we provide access to our Sites in a secure and effective way and so that we can make improvements to our Sites or it is necessary for us to use your personal data to perform our obligations in accordance with any contract that we may have with you for the Services.

We will collect and use personal data about you when you use certain features on our Site. For example, depending on the nature of your enquiry, we may process your Identity Data, Contact Data and certain Behavioural Data and Technical Data when you use the Enquiry Form to get in touch with us.

If you use the interactive features on our Site***Our legal basis for processing***

It is in our legitimate interest to use personal data in such a way to ensure that we can respond to your enquiries, provide access to our Sites in a secure and effective way and make improvements to our Site.

If you click on one of the social media links on our Sites or otherwise interact with our social media pages such as on Twitter or Instagram or YouTube (including interacting with any 'like' or similar embedded features on our Sites or social media accounts), we and the relevant social media platform may receive information relating to such interaction and may share your personal data in connection with this purpose, such as certain Behavioural Data and Technical Data. For more information about how we use this personal data, please see the "Insight, analysis and retargeting through Cookies" section below.

If you link to social media sites and interact with our social media pages

The relevant social media platform may also be a controller in respect of the personal data that is collected via your use of our social media pages and may use that personal data for additional purposes. For details of how the relevant social media platform uses your personal data, please see the privacy policy of the relevant social media platform.

Our legal basis for processing

It is in our legitimate interest to use personal data in the ways described above to ensure that we provide the Site in an effective way and to promote our Site via social media.

B: Fulfilment of our Services

Carrying out surveys and reporting

We collect and maintain personal data that you submit and/or third parties provide to us for in connection with your participation in one of our surveys that we carry out on behalf of our clients or for our own market analysis purposes.

The information you provide will normally be used to help a client better understand how they are doing in the marketplace, or to help them improve a service or similar. Data is typically presented back to our client as part of our Services in an aggregated, anonymised format, unless you consent to us providing them your Contact Data appended. For example, to enable you to collect a reward if completing a survey requires it.

The personal data we process may include your Identity Data, Contact Data, Respondent Data, and Financial Data (where applicable). We process this information so that we can fulfil the supply of our Services, maintain our user databases and to keep a record of how we provide our Services.

Our legal basis for processing

To the extent the above involves personal data and we are considered a controller of your data, it may be necessary for us to use your personal data to perform our obligations in accordance with any contract that we may have with you. Or it is in our legitimate interest or a third party's legitimate interest for us to use personal data in such a way to ensure that we provide the Services in an effective, safe and efficient way. Where we do this on behalf of our clients as a data processor, we do not require a legal basis for such processing.

We will not process any special (or sensitive) categories of personal data or personal data relating to criminal convictions or offences except where we are able to do so under applicable legislation or with your explicit consent.

Please note that often such services will relate to anonymous data sets (aggregated data sets, statistical data sets and similar) and are used for high-level market analytics or understanding macro consumer habits (amongst other things). When we do this, we and our clients are not processing personal data.

Managing our Panels

If you sign up to one of our market research opinion panels, we will process personal data about you which you provide to us when you complete your profile as part of the sign-up profile. This will usually include your Contact Data, Respondent Data, Financial Data and any other personal data you volunteer.

If you are a parent or guardian of a minor who signs up for a youth market research opinion panel, we may

also process your personal data to record that you have consented to the minor taking part in the panel and completing a profile. We may process this type of consent by recording a telephone call with you.

Once you have created a profile, we will be able to use this information provided to select you to take part in relevant surveys.

Our legal basis for processing

To the extent the above involves personal data, it may be necessary for us to use your personal data to perform our obligations in accordance with any contract that we may have with you. Or it is in our legitimate interest or a third party's legitimate interest for us to use personal data in such a way to ensure that we provide the Services in an effective, safe and efficient way.

In addition to providing bespoke market research services to clients, we can create aggregated and anonymised market insights through our Vue Product Range for our benefit and that of our clients using a wide range of software tools to extract information about target markets, customers, and marketing efforts from data provided to us by our clients or from information you provide to us through completing our

Provision of market insight through our Vue Product Range surveys or through third party providers.

Our legal basis for processing

To the extent the above involves personal data, it is in our legitimate interest or a third party's legitimate interest for us to use personal data in such a way to ensure our services are easy to use providing us and our clients with up to date and valuable insights. Where we do this on behalf of our clients as a data processor, we do not require a legal basis for such processing.

Use of our Vue Product Range.

You may be required to register an account with us in order to gain access to our Vue Product Range. Account applicants will need to complete the registration form, providing all required Identity Data and Contact Data (including their first name, last name, email address, telephone number, and organisation). We will use this data in order to process your registration.

Once the account is registered, we will process your Identity Data to identify you when you log in to your account and access secure areas of the Vue Product Range. We will also process certain Technical Data and Marketing and Communications Data so that we can administer your account and contact you about your account.

We will also collect and process Behavioural Data and Technical Data when you use certain features and functionality on our Vue Product Range. This data helps us understand how you use our Vue Product Range so that we can improve it.

Our legal basis for processing

It is necessary for us to use your personal data to perform our obligations in accordance with any contract that we may have with you, or it is in our legitimate interest to use personal data in such a way to ensure that we provide access to the Services in a secure and effective way and so that we can make improvements to our Services.

If you complete our surveys or provide feedback on your experience of our Site and/or our Services

From time to time, we will invite you to provide feedback about us, our Site and our Services in the form of online surveys. These are separate to the market research surveys we provide. We will collect and process your Identity Data and Contact Data as

well as any other personal data you choose to volunteer in your survey response or other feedback.

We use this information to help us to monitor and improve our Site and our Services, to assist with the selection of future service lines and to train our personnel.

You can also voluntarily provide feedback by email or via our [Enquiry Form](#).

Our legal basis for processing

It is in our legitimate interest to use the personal data provided by you so that we can improve our Site and our Services and provide them in an effective way.

From time to time, we may incentivize participation in our market research activities by running prize draws, prize competitions and other promotions on our Sites, client sites and/or on our social media accounts. For the purposes of administering such promotions, we may process your Identity Data, Contact Data and any other personal data volunteered by you in relation to your promotion entry.

If you participate in one of our promotions

Our promotions are subject to separate terms and conditions, which you may be required to accept as a condition of entry.

Our legal basis for processing

It is necessary for us to use your personal data to perform our obligations in accordance with any contract that we may have with you (e.g. the promotion terms and conditions) or it is in our legitimate interest to use your personal data to enable us to administer our promotion fairly and effectively and to ensure that we comply with self-regulatory codes governing the operation of promotions.

If you have a general question or need help with any issue concerning our Sites or our Services

There are various ways in which you are able to contact us (see the “How to Contact us” section above). In particular, our Site features a “Contact Us” page, which invites you to submit general enquiries about our Sites by email or via our [Enquiry Form](#). From time to time, you may also be able to submit specific enquiries on other pages of our Sites, including in secure account areas.

When you make an enquiry, we will collect and process your Identity Data, Contact Data as well as any other personal data you volunteer that is relevant to your enquiry. If you have a technical issue concerning our Sites, we may also collect and process Behavioural Data and Technical Data to help us diagnose the technical issues you are experiencing and to help us resolve them in an efficient way. We use this information to manage and respond to your enquiry.

We may record telephone conversations to improve how we train our personnel and the quality of our services.

Our legal basis for processing

It is in our legitimate interest to use your personal data in the ways described above to ensure that we are able to help you with your enquiry, provide a good standard of service and improve our customer services.

C: Hosting and managing

If you sign up for and/or attend one of our events

From time to time, we may organise and host events for the purpose of promoting our business or for charitable causes or other reasons. We may process your Identity Data and Contact Data to communicate with you about such events where you have specifically requested information about such events or where we have another lawful basis for sending that information to you.

If you attend one of our events, we may use your Identity Data and Contact Data to record your attendance at the event and for related record-keeping

purposes and, if relevant, we may collect and process any dietary requirements you may have. You may also feature in photographs taken at our events and such photographs may appear in publications that we make available.

Our legal basis for processing

It is necessary for us to use your personal data in this way to perform our obligations in accordance with any contract that we may have with you where you have signed up to attend an event, or it is in our legitimate interest or a third party's legitimate interest to use personal data in such a way to ensure that the event is operated in an effective way.

We may specifically ask your permission to use your photographs, quotes, testimonials, or other content that you make available or publish at the event. Where this is the case, our processing of your such personal data will be based on consent.

Get in touch

D: Insight, analysis and retargeting through Cookies

If we use cookies to help us understand more about you and your use of our Site and our Products and Services

We and our third-party partners use cookies, web beacons, pixel tags and other similar technologies (which we generically refer to as “**Cookies**”) to collect data from the devices that you use to access our Site and Services and any emails that you receive from . The data that is collected includes Behavioural Data and Technical Data Please see our [Cookie Policy](#) for further information, including details of our third-party partners.

We and our third-party partners use this data to analyse how you use our Sites and Services and the effectiveness of our Sites and Services, including:

- to count users who have visited our Sites or opened an email and collect other types of information, including insights about visitor browsing habits, which helps us to improve our Sites and Services and the effectiveness of our emails;

Latest Thinking

- to measure the effectiveness of our content;
- to learn what parts of our Sites are most attractive to our users, which parts of our Sites are the most interesting and what kind of features and functionalities our visitors like to see;
- to help us understand the type of marketing content that is most likely to appeal to our visitors and customers; and
- to help us with the selection of future service lines, website design and to remember your preferences.

In some of our email messages, we use a “click-through URL” linked to certain websites administered by us or on our behalf. We may track click-through data to assist in determining interest in particular topics and measure the effectiveness of these communications.

Our legal basis for processing

In certain circumstances, we may rely on another lawful basis when we use your personal data collected via the use of cookies. For example, where we use personal data collected through the use of analytics cookies to analyse how you use our Sites, it is in our legitimate interest to use your personal data in such a way to improve our Sites and Services.

E: Advertising and marketing activities

If we send you marketing communications by post and/or email/SMS

We use your Identity Data, Contact Data and Marketing and Communications Data to send you (or the organisation you represent) marketing communications by post and/or email/SMS. Our marketing will include press releases and information about us, our Site, our Services, any events we may hold and the offers and promotions we offer from time to time.

Our marketing communications will include personalised and non-personalised marketing.

Personalised marketing has been specifically tailored to you and will include content that we think is most relevant to you, based on what we know about you. Non-personalised marketing is marketing that is not tailored to you.

Where we are sending you personalised marketing, we may also use Transaction Data and Behavioural Data to help us decide what sort of personalised marketing to send you (please see the “Insight, analysis and retargeting through Cookies” section above for more details).

Our legal basis for processing

It is in our legitimate interest to use your personal data for marketing purposes, for example to decide what marketing content we think may appeal to you.

It is in our legitimate interest to use your personal data to send our marketing to you by post.

However, we will only send marketing communications to you by email and/or SMS where you have consented to receive such content by email and/or SMS, or where we have another lawful right to send marketing to you using email and/or SMS. For example, in certain circumstances we may rely on our legitimate interest to send marketing by email and/or SMS to consumers who have purchased our Services. We may also rely on our legitimate interest to send marketing by email and/or SMS to certain business users of our Sites and Services.

Blogs and Newsletters

We may also provide individuals with the opportunity to sign up for newsletters or to receive copies of blogs and other information that we make available. Where an individual signs up to receive such information, Contact Data may be requested as well as other information to ensure our communications are suitably tailored.

Our legal basis for processing

It is in our legitimate interests (and those of our clients) to process personal data in this way to ensure we provide the Services requested by our clients in an effective and efficient way and that we provide the right information to those who request it.

We may collect personal data (including Identity Data, Contact Data and Publicly Available Data) about journalists, client contacts or industry contacts for interview requests, for media questions, or requests for information about Savanta. This information is used in order to enable us to respond to individual requests or media requests.

Media and Informational inquiries

Our legal basis for processing

It is in our legitimate interests (and those of our clients) to process personal data in this way to ensure we provide the Services requested by our clients in an effective and efficient way and that we provide the right information to those who request it.

F: Recruitment

If we use your personal data in connection with our recruitment activities

We use your personal data for recruitment purposes, in particular, to assess your suitability for any of our positions that you apply for, whether such application has been received by us online, by email or by hard copy and whether submitted directly by you or by a third-party recruitment agency on your behalf. We also use your Identity Data and Contact Data to communicate with you about the recruitment process, to keep records about our recruitment process and to comply with our legal and regulatory obligations in relation to recruitment.

We will process any personal data about you that you volunteer, including during any interview, when you apply for a position with us. We may also process your personal data obtained from any third parties we work with in relation to our recruitment activities, including without limitation, recruitment agencies, background check providers, credit reference agencies and your referees.

The personal data we process may include your Identity Data, Contact Data, Job Application Data and any other personal data that you volunteer during an interview or your interactions with us, or any personal data which is contained in any reference about you that we receive. Such information may also include special categories of personal data (such as information about your health, any medical conditions and your health and sickness records) and information relating to criminal convictions and offences if that information is relevant to the role you are applying for.

We also use your personal data for the purposes of reviewing our equal opportunity profile in accordance with applicable legislation. We do not discriminate on the grounds of gender, race, ethnic origin, age, religion, sexual orientation, disability or any other basis covered by local legislation. All employment-related decisions are made entirely on merit.

Our legal basis for processing

Where we use your personal data in connection with recruitment and talent management, it will be in connection with us taking steps at your request to enter into a contract we may have with you, or it is in our legitimate interest to use personal data in such a way to ensure that we can make the best recruitment and talent management decisions.

We will not process any special (or sensitive) categories of personal data or personal data relating to criminal convictions or offences except where we are able to do so under applicable legislation or with your explicit consent.

G: Receipt of products and services from our suppliers

If we have engaged you or the organisation you represent to provide us with products or services

If we have engaged you or the organisation you represent to provide us with products or services (for example, if you or the organisation you represent provide us with services such as IT support or financial advice), we will collect and process your personal data in order to manage our relationship with you or the

organisation you represent, to receive products and services from you or the organisation you represent and, where relevant, to provide our Services to others. The personal data we collect from you may include your Identity Data and Contact Data and any other personal data you volunteer which is relevant to our relationship with you or the organisation you represent.

Our legal basis for processing

It is necessary for us to use your personal data to perform our obligations in accordance with any contract that we may have with you or the organisation you represent, or it is in our legitimate interest to use personal data in such a way to ensure that we have an effective working relationship with you or the organisation you represent and are able to receive the products and services that you or your organisation provides, and provide our Services to others, in an effective way.

H:

We have security measures in place at our premises, including CCTV and building access controls. There are signs in place showing that CCTV is in operation. The images captured are securely stored and only accessed on a need-to-know basis (e.g. to look into an incident). CCTV recordings are typically automatically overwritten after a short period of time unless an issue is identified that requires investigation (such as a theft).

If we need to use your personal data in connection with the administration of our security measures

We may require visitors to our premises to sign in on arrival and where that is the case, we will keep a record of visitors for a short period of time. Our visitor records are securely stored and only accessible on a need-to-know basis (e.g. to look into an incident).

Our legal basis for processing

It is in our legitimate interests to process your personal data so that we can keep our premises secure and provide a safe environment for our personnel and visitors to our premises.

Get in touch

Latest Thinking

I: Business administration and legal compliance

We may use your personal data: (i) to comply with our legal obligations; (ii) to enforce or protect our legal rights; (iii) to protect the rights of third parties; and (iv) in connection with a business transition such as a merger, reorganisation, acquisition by another company, or sale of any of our assets.

Our legal basis for processing

If we need to use your personal data to comply with our legal obligations or in connection with the administration of our business

Where we use your personal data in connection with a business transition, to enforce or protect our legal rights or to protect the rights of third parties, it is in our legitimate interest to do so. For all other purposes described in this section, we have a legal obligation to use your personal data to comply with any legal obligations imposed upon us, such as a court order.

We will not process any special (or sensitive) categories of personal data or personal data relating to criminal convictions or offences except where we are able to do so under applicable legislation or with your explicit consent.

9 If you fail to provide your personal data

Where we are required by law to collect your personal data, or we need to collect your personal data under the terms of a contract we have with you, and you fail to provide that personal data when we request it, we may not be able to perform the contract we have or are trying to enter into with you. This may apply where you do not provide the personal data we need in order to provide the Services you have requested from us or to process an application for employment with us. In these circumstances, we may have to cancel your application or the provision of the relevant Services to you, in which case we will notify you.

10 How we obtain your consent

Where our use of your personal data requires consent, you can provide such consent at the time we collect your personal data following the instructions provided, or by informing us using the contact details set out in the “How to Contact Us” section above.

11 Third-party links

This Privacy Notice only applies to personal data processed by us through your use of our Sites and/or in connection with our business operations. However, from time to time, our Sites may contain links to third-party websites and services. We have no control over these websites and services and this Privacy Notice does not apply to your interaction with the relevant third parties.

When you use a link to go from our Site to another website (even if you don't leave our Site) or you request a service from a third party, your browsing and interactions on any other websites, or your dealings with any other third-party service provider, is subject to that website's or third-party service provider's own rules and policies. For example, our Site invites you to connect with us on social media platforms such as Twitter and LinkedIn. When you click on the links we provide to such third-party platforms, you will be transferred from our Site to the relevant third-party platform and the privacy notice (and other terms and conditions) of that platform will apply to you.

We do not monitor, control or endorse the privacy practices of any third parties. We encourage you to become familiar with the privacy practices of every website you visit or third-party service provider that you use in connection with your interaction with us and to contact them if you have any questions about their respective privacy notices and practices.

12 Sharing Your personal data

We only share personal data with others when we are legally permitted to do so. When we share personal data with others, we put contractual arrangements and security mechanisms in place to protect the personal data shared and to comply with our data protection, confidentiality and security standards and obligations.

When processing your personal data, we may need to share it with third parties (including other entities within our group of companies), as set out in the table below. This list is non-exhaustive and there may be circumstances where we need to share personal data with other third parties.

Our clients	We may share personal data with our clients for the purposes of providing them with our Services.
Our specialist suppliers/partners	We use various specialist suppliers and/or partners in order to provide our Services including sample suppliers.
Third-party suppliers who provide applications/ functionality, data processing or IT services	We share personal data with third parties who support us in providing our Sites and help provide, run and manage our internal IT systems. Such third parties may also include, for example, providers of information technology, cloud-based software-as-a-

Get in touch

Latest Thinking

	<p>service providers, identity management, website design, hosting and management, data analysis, data back-up, security and storage services. The servers powering and facilitating that cloud infrastructure are located in secure data centres around the world, and personal data may be stored in any one of them. We also share your personal data with third-party service providers to assist us with insight analytics. These providers are described in our Cookie Policy.</p>
Payment providers and banks	<p>We share personal data with third parties who assist us with the processing of payments and refunds.</p>
Third-party post/email marketing and CRM specialists	<p>We share personal data with specialist suppliers who assist us in managing our marketing database and sending out our post and email marketing communications and account-related communications.</p>
Third-party suppliers who assist us in administering our promotions	<p>We share personal data with specialist suppliers who assist us in administering our prize draws, prize competitions and other promotions.</p> <p>When we run events, we will share your personal data with third-party service providers that are assisting us with the operation and administration of that event. If we are running an event in partnership with other organisations, we will share your personal data with such organisations for use in relation to the event.</p>
Event partners and suppliers	<p>We share personal data with external recruiters, third-party providers that undertake background checks on our behalf and other entities within our group of companies.</p>
Recruitment agencies and related organisations	<p>We share personal data with professional services firms who advise and assist us in relation to the lawful and effective management of our organisation and in relation to any disputes we may become involved in.</p>
Auditors, lawyers, accountants and other professional advisers	<p>We share personal data with law enforcement or other government and regulatory agencies or other third parties as required by, and in accordance with, applicable law or regulation.</p>
Law enforcement or other government and regulatory agencies and bodies	<p>Occasionally, we may receive requests from third parties with authority to obtain disclosure of personal data, such as to check that we are complying with applicable law and regulation, to investigate an alleged crime, or to establish, exercise or defend legal rights. We will only fulfil requests for personal data where we are permitted to do so in accordance with applicable law or regulation.</p>
Other third parties	

In respect of personal data that we process in connection with the supply of our Services, we may retain your personal data for up to seven years from the date of supply of the relevant Services and in compliance with our data protection obligations. We may then destroy such files without further notice or liability.

Where we process personal data in connection with the registration and use of an account on our Sites, we may retain your personal data for up to seven years from the date that the relevant account is terminated (and in compliance with our data protection obligations). We may then destroy such files without further notice or liability.

Where we process any other personal data, we will retain relevant personal data for up to three years from the date of our last interaction with you (and in compliance with our data protection obligations). We may then destroy such files without further notice or liability.

If any personal data is only useful for a short period (e.g. for a specific market research activity, promotion or marketing campaign), we will not retain it for longer than the period for which it is used by us.

If you have opted out of receiving marketing communications from us, we will need to retain certain personal data on a suppression list indefinitely so that we know not to send you further marketing communications in the future. However, we will not use this personal data to send you further marketing unless you subsequently opt back in to receive such marketing.

14 Confidentiality and security of your personal data

We are committed to keeping the personal data you provide to us secure and we have implemented information security policies, rules and technical measures to protect the personal data under our control from unauthorised access, improper use or disclosure, unauthorised modification and unlawful destruction or accidental loss. In addition, all our employees and data processors (i.e. those who process your personal data on our behalf) are obliged to respect the confidentiality of the personal data of all users of our Site and those who purchase our Services.

15 Personal data of minors

We may process personal data of minors (individuals aged 13 to 18 years old) in connection with the provision of our Services including through our youth service. We rely on the lawful bases set out above to process such personal data and where legally required we will obtain parental consent in order to process such personal data.

16 Your rights as a data subject

You have certain rights in relation to the personal data we hold about you. These rights include the right: (i) to obtain copies of your personal data; (ii) to have your personal data corrected or deleted; (iii) to limit the way in which your personal data is used; (iv) to object to our use of your personal data; (v) to transfer your personal data; (vi) not to be subject to decisions based on automated processing (including profiling); and (vii) to complain to a supervisory authority. If you would like to exercise any of these rights, please contact us using the details set out in the “above.

For more information about your specific data subject rights in certain jurisdictions, please see relevant jurisdiction specific section below.

17 COUNTRY SPECIFIC PROVISIONS

UNITED KINGDOM (“UK”) AND EUROPEAN ECONOMIC AREA (“EEA”)

This UK and EEA Privacy Statement supplements the Savanta Privacy Notice. It applies to the extent our processing of your data is caught by the requirements of the UK GDPR and/or EU GDPR.

Transfers outside the UK and the European Economic Area (“EEA”)

We may transmit personal data outside the UK and EEA to certain categories (as listed above in Sharing your Personal Data and more specifically to (1) our headquarters in San Francisco (“US”); (2) Savanta Group entities, networks or partner agencies in for example, India and other locations globally.

Therefore, when you submit personal data to us, whether through your interactions with our Site, and branch offices or our headquarters in the US, you acknowledge that your personal data will be transferred outside the UK and the EEA to the US and other global locations where it will be stored and processed by us and our suppliers for the purposes set out in this Privacy Notice.

Where necessary in order to provide our Site and our Services, we will transfer personal data to countries outside the UK and the EEA.

Non-EEA countries do not have the same data protection laws as the UK and the EEA. In particular, non-EEA countries may not provide the same degree of protection for your personal data, may not give you the same rights in relation to

your personal data and may not have a data protection supervisory authority to help you if you have any concerns about the processing of your personal data.

However, when transferring your personal data outside the UK or the EEA, we will comply with our legal and regulatory obligations in relation to your personal data, including having a lawful basis for transferring personal data and putting appropriate safeguards in place to ensure an adequate level of protection for the personal data. We will take reasonable steps to ensure the security of your personal data in accordance with applicable data protection laws.

When transferring your personal data outside the UK or the EEA, we will, where required by applicable law, implement at least one of the safeguards set out below. Please contact us if you would like further information on the specific mechanisms used by us when transferring your personal data outside the UK or the EEA.

Adequacy decisions	We may transfer your personal data to countries that have been deemed to provide an adequate level of protection for personal data by the European Commission and/or the UK Government (as applicable).
Standard Contractual Clauses	Where we use certain service providers, we may use specific standard contractual clauses approved by the European Commission and/or the UK Government which give personal data the same protection it has in Europe and/or the UK.

Your rights as a data subject

To the extent our processing of your data as a Data Controller is caught by the UK GDPR and/or EU GDPR, you have the following rights. If you would like to exercise any of these rights, please contact us using the details set out in the “How to Contact Us” section above.

Your right of access	If you ask us, we will confirm whether we are processing your personal data and, if so, provide you with a copy of that personal data (along with certain other details). If you require additional copies, we may charge a reasonable fee for producing those additional copies.
Your right to rectification	If the personal data we hold about you is inaccurate or incomplete, you are entitled to have it rectified. If we have shared your personal data with others, we'll let them know about the rectification where possible. If you ask us, where possible and lawful to do so, we will

Your right to erasure

also tell you who we've shared your personal data with so that you can contact them.

You can ask us to delete or remove your personal data in some circumstances, such as where we no longer need it or where you withdraw your consent (where applicable). If we have shared your personal data with others, we will let them know about the erasure where possible. If you ask us, where it is possible and lawful for us to do so, we will also tell you who we have shared your personal data with so that you can contact them directly.

Your right to restrict processing

You can ask us to "block" or suppress the processing of your personal data in certain circumstances such as where you contest the accuracy of that personal data or you object to us processing it for a particular purpose. This may not mean that we will stop storing your personal data but, where we do keep it, we will tell you if we remove any restriction that we have placed on your personal data to stop us processing it further. If we've shared your personal data with others, we'll let them know about the restriction where it is possible for us to do so. If you ask us, where it is possible and lawful for us to do so, we'll also tell you who we've shared your personal data with so that you can contact them directly.

Your right to data portability

You have the right, in certain circumstances, to obtain personal data you have provided to us (in a structured, commonly used and machine-readable format) and to reuse it elsewhere or to ask us to transfer it to your chosen third party.

Your right to object

You can ask us to stop processing your personal data, and we will do so, if we are: (i) relying on our own or someone else's legitimate interest to process your personal data, except if we can demonstrate compelling legal grounds for the processing; or (ii) processing your personal data for direct marketing purposes.

Your rights in relation to automated decision-making and profiling

You have the right not to be subject to a decision when it is based on automatic processing, including profiling, if it produces a legal effect or similarly significantly affects you, unless such profiling is necessary for the entering into, or the performance of, a contract between you and us.

Your right to withdraw consent

If we rely on your consent (or explicit consent) as our legal basis for processing your personal data, you have the right to withdraw that consent at any time. You can exercise your right of withdrawal by contacting us using our contact details in the "How to Contact Us" section above or by using any other opt-out



Your right to lodge a complaint with the supervisory authority

mechanism we may provide, such as an unsubscribe link in an email.

If you have a concern about any aspect of our privacy practices, including the way we have handled your personal data, please contact us using the contact details provided in the “How to Contact Us” section above. You can also report any issues or concerns to a national supervisory authority in the Member State of your residence or the place of the alleged infringement. You can find a list of contact details for all EU supervisory authorities at

As we are incorporated in the United Kingdom, our regulatory authority is the Information Commissioner’s Office (“ICO”). Contact details for the ICO can be found on its website at <https://ico.org.uk>.

UNITED STATES**California Consumer Privacy Statement**

This California Consumer Privacy Statement (“Statement”) supplements the [Savanta Privacy Notice](#). It applies solely to California consumers and addresses personal information we collect online and offline. This Statement does not apply to Savanta personnel. Sections 2-5 of this Statement do not apply to job applicants.

This Statement uses certain terms that have the meaning given to them in the California Consumer Privacy Act of 2018 and its implementing regulations (the “CCPA”).

1. Notice of Collection and Use of Personal Information

We may collect (and may have collected during the 12-month period prior to the effective date of this Statement) the following categories of personal information about you:

Identifiers: identifiers such as a real name, alias, postal address, unique personal identifier (such as a device identifier; cookies,

beacons, pixel tags, mobile ad identifiers and similar technology; customer number, unique pseudonym, or user alias; telephone number and other forms of persistent or probabilistic identifiers), online identifier, internet protocol address, email address, account name, Social Security number, driver's license number, passport number, and other similar identifiers

Additional Data Subject to Cal. Civ. Code § 1798.80: signature, physical characteristics or description, state identification card number, insurance policy number, education, bank account number, credit card number, debit card number, and other financial information, medical information, and health insurance information

Protected Classifications: characteristics of protected classifications under California or federal law, such as race, color, national origin, religion, age, sex, gender, gender identity, gender expression, sexual orientation, marital status, medical condition, ancestry, genetic information, disability, citizenship status, and military and veteran status

Commercial Information: commercial information, including records of personal property, products or services purchased, obtained, or considered, and other purchasing or consuming histories or tendencies

Online Activity: Internet and other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding your interaction with websites, applications or advertisements

Sensory Information: audio, electronic, visual, and similar information

Employment Information: professional or employment-related information

Education Information: education information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. Sec. 1232g; 34 C.F.R. Part 99)

Inferences: inferences drawn from any of the information identified above to create a profile about you reflecting your preferences, characteristics, psychological trends, predispositions, behaviour, attitudes, intelligence, abilities, and aptitudes.

We may use (and may have used during the 12-month period prior to the effective date of this Statement) your personal information for the purposes described in our [Privacy Notice](#) and for the following business purposes specified in the CCPA:

Performing services, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing advertising or marketing services, providing analytics services, or providing similar services

Auditing related to a current interaction with you and concurrent transactions, including, but not limited to, counting ad impressions to unique visitors, verifying positioning and quality of ad impressions, and auditing compliance

Short-term, transient use, including, but not limited to, the contextual customization of ads shown as part of the same interaction

Detecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, and prosecuting those responsible for that activity

Debugging to identify and repair errors that impair existing intended functionality

Undertaking internal research for technological development and demonstration

Undertaking activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by us, and to improve, upgrade, or enhance the service or device that is owned, manufactured, manufactured for, or controlled by us.

Managing career opportunities with Savanta.

1. Sources of Personal Information

During the 12-month period prior to the effective date of this Statement, we may have obtained personal information about you from the following categories of sources:

- Directly from you, such as when you contact us with a question or comment
- From your devices, such as when you visit our Site
- Vendors who provide services on our behalf
- Social networks
- Government entities
- Data brokers

1. Sale of Personal Information

We do not and will not sell your personal information.

1. Sharing of Personal Information

During the 12-month period prior to the effective date of this Statement, we may have shared your personal information with certain categories of third parties, as described below.

We may have disclosed the following categories of personal information about you for a business purpose to the following categories of third parties:

Category of Personal Information	Category of Third Party
Identifiers	Our affiliates and subsidiaries; Vendors who provide services on our behalf; Professional services organizations, such as auditors and law firms; Our business partners; Advertising networks; Internet service providers; Data analytics providers; Operating systems and platforms; Social networks
Additional	Our affiliates and subsidiaries; Vendors who provide services on our behalf; Professional services

Get in touch

Latest Thinking

	organizations, such as auditors and law firms; Our business partners; Advertising networks; Internet service providers; Data analytics providers; Operating systems and platforms; Social networks Our affiliates and subsidiaries; Vendors who provide services on our behalf; Professional services
Protected Classifications	organizations, such as auditors and law firms; Our business partners; Advertising networks; Internet service providers; Data analytics providers; Operating systems and platforms; Social networks Our affiliates and subsidiaries; Vendors who provide services on our behalf; Professional services
Commercial	organizations, such as auditors and law firms; Our business partners; Advertising networks; Internet service providers; Data analytics providers; Operating systems and platforms; Social networks Our affiliates and subsidiaries; Vendors who provide services on our behalf; Professional services
Online Activity	organizations, such as auditors and law firms; Our business partners; Advertising networks; Internet service providers; Data analytics providers; Operating systems and platforms; Social networks Our affiliates and subsidiaries; Vendors who provide services on our behalf; Professional services
Employment Information	organizations, such as auditors and law firms; Our business partners; Advertising networks; Internet service providers; Data analytics providers; Operating systems and platforms; Social networks Our affiliates and subsidiaries; Vendors who provide services on our behalf; Professional services
Education Information	organizations, such as auditors and law firms; Our business partners; Advertising networks; Internet service providers; Data analytics providers; Operating systems and platforms; Social networks Our affiliates and subsidiaries; Vendors who provide services on our behalf; Professional services
Inferences	organizations, such as auditors and law firms; Our business partners; Advertising networks; Internet service providers; Data analytics providers; Operating systems and platforms; Social networks

In addition to the categories of third parties identified above, during the 12-month period prior to the effective date of this Statement, we may have shared personal information about you with the following additional categories of third parties:

Government entities.

1. California Consumer Privacy Rights

Get in touch

Latest Thinking

You have certain choices regarding our use and disclosure of your personal information, as described below.

Access: You may have the right to request, twice in a 12-month period, that we disclose to you the personal information we have collected, used, disclosed and sold about you during the past 12 months.

Deletion: You have the right to request that we delete certain personal information we have collected from you.

How to Submit a Request: To submit an access or deletion request (or to submit a request as an authorized agent on behalf of a consumer), please contact us as described in “How to Contact Us” section above.

Verifying Requests: To help protect your privacy and maintain security, we will take steps to verify your identity before granting you access to your personal information or complying with your request. If you request access to or deletion of your personal information, we may require you to provide any of the following information: your email address, the name of the Savanta representative with whom you typically interact, and the date of your last interaction with a Savanta representative. In addition, if you ask us to provide you with specific pieces of personal information, we will require you to sign a declaration under penalty of perjury that you are the consumer whose personal information is the subject of the request.


Additional Information: If you choose to exercise any of your rights under the CCPA, you have the right to not receive discriminatory treatment by us. To the extent permitted by applicable law, we may charge a reasonable fee to comply with your request.




[Terms & conditions](#) [Cookie policy](#) [Privacy policy](#) [Data protection](#)
[Accessibility statement](#) [Carbon Reduction Plan](#) [Modern Slavery Statement](#)

Savanta Group 2024

Registered in Scotland (SC 281 352) | Registered Address: C/O Bellwether Green
Limited, 225 W George St, Glasgow G2 2ND

 Get in touch

 Latest Thinking



Privacy Policy

I. PRIVACY POLICY

This privacy policy is effective as of October 5, 2022. MFour Mobile Research, Inc. ("MFour," "we," "us," "our") is committed to protecting the privacy and security of your personal information. We also want to be upfront and clear about information we collect, how we use it, and rights you may have. MFour is a market research technology company providing services, including sharing data, to other market research companies, third parties operating in the ad tech sector, companies providing products and services to consumers, and other parties (collectively "Partners") for the purposes of market research, including ad measurement, analytics and reporting, and other purposes. MFour does not share data with Partners that would use the data to directly advertise or market to you.

This Privacy Policy explains how we collect, use, and share information when individuals ("you") visit or interact with our websites including www.surveyonthego.com, www.surveyonthego.net, www.mfour.com, and www.mfour.net (the "Sites"), and the Surveys On The Go® mobile application (the "SOTG App"). The Sites and the SOTG App together are called the "Services" in this Privacy Policy.

The SOTG App is available in the Apple App Store and Google Play Store. If you download the SOTG App, you will be able to create an account and receive and respond to surveys that we conduct for our use or on behalf of our Partners. We offer you incentives in exchange for your survey participation. As explained in more detail below, we share survey results and other information collected through the SOTG App with our Partners who typically use the information we provide to conduct and improve their products, services, and advertising. From time to time, we may permit selected third parties to provide you with additional survey opportunities in the SOTG App. If you decide to participate in those additional opportunities, your participation in those third-party surveys will be directly with those third parties and will not be governed by this Privacy Policy.



1. Types of information collected and how we collect them

Personal information you provide to us

When you use the Services, we collect personal information that you provide to us. This information may include your name, address, telephone number, email address, and linked information such as zip code, demographic information (such as your age, gender, income, education level, etc.), and other information. We collect this information when you voluntarily provide it to us when creating an account after downloading the SOTG App, when you use the SOTG App to update your account information, and when you respond to surveys.

We will use demographic and other information you provide to send you relevant surveys and for other internal purposes. If you participate in a survey, we will collect information and responses that you provide in the course of the survey. For some surveys, this may include photo, audio, and video information that you provide. If you use our Facebook log-in tool, we may collect the information you choose to make publicly available through your Facebook profile such as your name, date of birth, email address, and residence location. You can control what specific information is made public through your use of your Facebook privacy settings.

Personal information collected automatically

We collect certain personal information automatically through the SOTG App and when you visit the Sites. Geographic Location Information and Digital Data (described below) will be collected automatically only if you give permission. Personal information that is automatically collected includes the following:

Geographic Location Information. If permitted on your device and with your permission, the SOTG App may automatically collect and use your Geographic Location Information, which includes precise location information from your device.

You will receive prior notice and must give your consent before your Geographic Location Information is collected through the SOTG App (in the event that you share your device with another person, please be aware that this person could change these permissions on your behalf). If you do not want to provide your Geographic Location Information through the SOTG App, you may use the controls available in the SOTG App and/or available on your mobile device to limit this sharing. Some incentives and features may not be available if you stop the collection of Geographic Location Information.



data they collect, to make it easier for you to navigate our Services, to provide a better experience for you when you participate in surveys, and for quality control and validation purposes. Cookies are small text files or other forms of data which are stored on a computer by a website and can store certain information about the internet browsing activity on that computer. You may be able to disable and/or delete cookies via your browser and/or plug-in settings; however, this may: (1) decrease the functionality of our Sites and other websites you visit; (2) limit your ability to use and view our Services; and (3) limit your participation in the Services, including incentivized surveys. Even if you disable cookies, we may collect and use other information that identifies your device over time to provide our Services.

The information we collect automatically when you visit the Sites or use the Services includes, for example, IP address, pages visited and other activities on the Services, information about your other online activities, streaming video services you use and the content you watch, general geographic location derived from IP address, and time and date of your activities. We also collect information about your device and its software, such as your mobile advertising identifier, device manufacturer, device type, device model, operating system and version, browser type, wireless carrier/provider information, Internet service provider, and a randomized unique ID (that allows us to uniquely identify your browser, mobile device, or SOTG account).

Digital Data. If permitted on your device and with your permission, the SOTG App may automatically collect Digital Data about your other online activities outside the SOTG App, including webpages you visit on the device, apps that you use on the device, information about how and for how long you use the apps, and apps that you install and uninstall. The Digital Data collected also includes activities and purchases you make on e-commerce apps and websites.

To provide Digital Data, you must enable accessibility permissions on Android devices and download a Virtual Private Network (VPN) tool on iOS devices. If you want to stop providing Digital Data through the SOTG App, you can use the controls available in the SOTG App and/or available on your mobile device to disable the collection of Digital Data. You may also stop providing Digital Data by disabling accessibility permissions on Android devices or disabling and/or uninstalling the VPN on iOS devices. Some incentives and features may not be available as a result of stopping the collection of Digital Data.

Personal information from third parties



other information.

We may also use analytics services provided by third parties. These service providers may use cookies or other technologies to collect information about your online activities on the Sites, the SOTG App, and other sites and apps over time for analytics purposes. For example, we use Google Analytics to understand how visitors use our Sites. For more information from Google about how Google Analytics collects and uses data, visit <https://www.google.com/policies/privacy/partners> (<https://www.google.com/policies/privacy/partners>). To opt out of Google Analytics, visit <https://tools.google.com/dlpage/gaoptout> (<https://tools.google.com/dlpage/gaoptout>).

2. Payday Program

Payday is an optional program that allows you to receive a weekly incentive in addition to survey incentives. If you choose to participate in Payday, you may also receive more surveys. In order to be eligible for Payday, you must consent to and allow us to automatically collect Geographic Location Information and Digital Data as described above. We will use and share this information as described in this Privacy Policy. You will automatically be eligible for a Payday incentive if you provide Geographic Location Information and Digital Data for at least 15 days during a month and log into the SOTG app at least once during a month. Even if you do not participate in Payday, we may still collect, use, and share information through the Services as described in other sections of this Privacy Policy.

You can permanently disable or temporarily pause the collection of Geographic Location Information and/or Digital Data at any time, but stopping this data collection will affect your eligibility for a Payday incentive. If you want to stop providing Geographic Location Information and/or Digital Data to us through the SOTG App, you can use the controls available in the SOTG App and/or available on your mobile device. You may also stop providing Digital Data by disabling accessibility permissions on Android devices and disabling and/or uninstalling the VPN on iOS devices. Some incentives and features may not be available as a result of stopping the collection of Digital Data. Pausing or disabling our collection of Geographic Location Information and/or Digital Data will not pause or disable any other data collection through our Services, and you will continue to receive surveys through the SOTG App. For California residents, please see below for our Notice of Financial Incentive for SOTG including the Payday program.

3. How we use and retain personal information



Information we collect for:

- Providing you with relevant survey opportunities. For example, demographic information may be used to match you to types of consumers a Partner may want to survey. Or, your location data may be used to offer you surveys while you are visiting a specific location such as a store or restaurant.
- Market research, including sharing data with our Partners as further described in the next section.
- Conducting our research and analysis to improve our products and services, identify consumer trends, develop consumer segments and other market research purposes.
- Our compliance with laws and legal obligations and maintaining the security of our Services and your information.
- Detecting and preventing fraudulent users of the Services and survey responses and other fraudulent activities.
- Paying incentives to you using your email address or other information.
- Communicating with you such as responding to your comments or questions, authenticating your identity, and providing you with updates to our products and services.
- Monitoring, administering, and enhancing our Services, including troubleshooting, data analysis, testing, research, statistical, and survey purposes.

We retain your SOTG App account information over time in order to provide the Services to you, including to offer you additional survey opportunities for Partners or for our internal research.

4. Disclosures of personal information

We want you to understand when and with whom we share your personal information. We may disclose your personal information in the ways described below. When we sell or otherwise provide personal information to our Partners, we restrict them by contract from using personal information collected through the SOTG App for direct marketing or advertising of products or services back to you.

- *To our Partners, which handle the information according to their own privacy policies.* We share information with our Partners to provide them with our services or for their own purposes. Typically, the information we share with Partners can include personal information, survey responses, Geographic Location



data. We may also permit selected third parties to collect and use your Geographic Location information through our SOTG App to provide you additional survey opportunities from those third parties.

- *Authorized third-party vendors and service providers.* In some cases, we share information we collect with authorized contractors, subcontractors, vendors, and service providers who help us operate our business and provide the Services. For example, we may share personal information with service providers that provide services such as web hosting, data analysis and reporting, auditing and compliance, network and data security, and identifying consumer demographics and geolocation.
- *Legal purposes.* We disclose personal information when we believe in good faith that the law requires it, pursuant to a court order, subpoena, warrant, in response to a law enforcement request, or as otherwise required or requested by law, regulation, or government authority programs; when disclosing this information is necessary to identify, contact or bring legal action against someone who may be violating the law or our rights or interfering with (either intentionally or unintentionally) use of Services or to protect our rights or the rights or safety of others; and for other legal related purposes.
- *Business event.* We may disclose personal information in connection with an actual or potential sale of stock or assets, merger, or any other change of control transaction (including in bankruptcy), or in the case of a bulk or partial sale, or other transfer (including third party panelist administration) of information to another research organization or entity.
- *With your consent.* We share personal information for any other purpose disclosed to you with your consent.

We may also share and disclose information that is aggregated, de-identified, or otherwise does not specifically identify you or your device, in our discretion including to our Partners.

5. Third-party links & tools

Our Services may provide links to third-party websites or apps, including offers and links to additional survey opportunities on third-party platforms. We do not control the privacy practices of those websites or apps, and they are not covered by this Privacy Policy. You should review the privacy policies of other websites or apps to learn about their data practices.



snaring such information with us and the general public. Your interactions with third-party companies and your use of their features are governed by the privacy notices of the companies that provide those features.

We encourage you to carefully read the privacy notices of any accounts you create and use.

6. Updating your personal information, deactivating your SOTG account, and stopping information collection

If you have a SOTG App account, you can review, change, or update some of your account information under the "Profile" tab in the SOTG App.

You can also ask us to delete your personal information related to your SOTG App account from our active files by emailing us at support@surveysonthego.net (<mailto:support@surveysonthego.net>). We may still retain some personal information as needed for legal and recordkeeping purposes, where permitted by law. A request to delete your personal information will not affect any information that we previously shared with Partners or other third parties as described above. In all other cases, we will retain information as long as required by law or as long as needed for our business purposes.

If you no longer want us to collect information from you via the SOTG App, you can stop responding to surveys and delete and uninstall the SOTG App from your device. We will keep your account information in our records in case you want to reinstall the SOTG Application and reactivate your account. We may also continue to use and share the information that you previously provided, as described in this Privacy Policy.

7. Minors under 16

We do not knowingly collect or sell personal information about individuals under the age of 16. If we learn that a person under 16 has provided us with personal information, we will endeavor to delete that information from our database. If you are a parent or legal guardian and believe that your child who is under 16 may have given us personal information, please contact us.

8. Nevada privacy rights



[sell-my-info/](#)).

- Toll-free telephone call. You may submit requests by calling our toll-free request line at 1-800-418-9018
- In the SOTG App. If you have an account with us, you may submit requests using the Privacy Center in the SOTG App. The Privacy Center is in the Profiles section of the SOTG App.

9. California privacy rights

This section contains disclosures required by the California Consumer Privacy Act ("CCPA") and applies only to "personal information" that is subject to the CCPA.

Personal Information We Collect.

In the past 12 months, we collected the categories of personal information about California consumers listed below:

- Personal and online identifiers such as first and last name, email address, postal address, or IP address;
- Characteristics of legally protected classifications(such as race or gender);
- Commercial or transactions information (such as records of personal property or products or services purchased, obtained, or considered);
- Internet or other electronic network activity information (such as browsing history, search history, or interactions with a website, email, application, or advertisement);
- Usage and device data;
- Audiovisual information (such as photos, videos, and voice recordings);
- Geolocation information;
- Education information;
- Inferences drawn from the above information about your predicted characteristics and preferences;
- Other information about you that is linked to the personal information above.



- Partners (as defined in this Privacy Policy);
- Social networks;
- Service providers;
- Consumer data resellers.

Our Purposes for Processing Personal Information. We collect, use, and disclose (including selling) the personal information we collect for our commercial and business purposes, as further described in this Privacy Policy.

Recipients of California Personal Information.

During the past 12 months, we disclosed, shared, or sold each category of personal information we collected to the categories of third parties listed below.

- Partners (as defined in this Privacy Policy);
- Service providers.

Your Rights Regarding Personal Information.

California residents have certain rights with respect to the personal information collected by businesses. If you are a California resident, you may exercise the following rights regarding your personal information, subject to certain exceptions and limitations:

- The **right to know** the categories and specific pieces of personal information we collect, use, disclose, and sell about you, the categories of sources from which we collected your personal information, our purposes for collecting or selling your personal information, the categories of your personal information that we have either sold or disclosed for a business purpose, and the categories of third parties with which we have shared personal information;
- The **right to request that we delete** the personal information we have collected from you.
- The right to **opt out of our sale(s)** of your personal information. Please note that if you opt out of certain types of sales, we will be unable to provide you with the services that rely on such sales, including survey opportunities.



verifying information, as further described below:

- Using this link. <https://surveysonthego.com/do-not-sell-my-info/> (<https://surveysonthego.com/do-not-sell-my-info/>).
- Toll-free telephone call. You may submit requests by calling our toll-free request line at 1-800-418-9018
- In the SOTG App. If you have an account with us, you may submit requests using the Privacy Center in the SOTG App. The Privacy Center is in the Profiles section of the SOTG App.

Verification Process and Required Information.

Note that we may need to request additional information from you to verify your identity or understand the scope of your request, although you will not be required to create an account with us to submit a request or have it fulfilled. You may be required to provide the following for verification purposes:

- Your first and last name
- Your email address
- Your telephone number

Authorized Agent.

You may designate an authorized agent to make a CCPA request on your behalf by providing us with a power of attorney or your written permission to allow the authorized agent to submit the request on your behalf and verification of your identity.

10. Notice of Financial Incentive for California Residents

Through the SOTG App, we provide you with opportunities to receive payments in exchange for providing data and/or responding to surveys. Through our surveys and the SOTG App, we may collect and share your personal information as described in this Privacy Policy. This includes all categories of personal information listed in Section 8 of this Privacy Policy.

The terms associated with each survey, like the amount you will receive if you qualify for and complete the survey, are presented to you in the SOTG App. Additional incentives may be available if you give permission for us to collect and share Geographic Location Information and Digital Data, including by participating in the



You opt into these financial incentives by participating in surveys and/or allowing us to collect Geographic Location Information and/or Digital Data. California residents have the right to withdraw from the financial incentives we offer at any time. You can pause or disable our collection of Digital Data and/or Geographic Location Information by using controls available in the SOTG App and/or your mobile device. You may also stop providing Digital Data by disabling accessibility permissions on Android devices and disabling and/or uninstalling the VPN on iOS devices. Pausing or disabling our collection of Geographic Location Information and/or Digital Data will not pause or disable any other data collection through our Services, and you will continue to receive surveys through the SOTG App. You can withdraw from survey participation by not responding to surveys or deleting the SOTG App from your mobile device.

The amount of payment you receive for completing a survey and/or providing data is based on the reasonable determination of the value that we and our partners receive from processing personal information. This estimated value takes into account a variety of factors as permitted by law, including (but not limited to) the expenses incurred in collecting and retaining the information, the expenses incurred in providing payments to you, and the estimated marginal revenue derived from information related to our surveys.

11. Changes to our privacy policy

We reserve the right to modify or revise this Privacy Policy at any time and in our sole discretion. We will post any changes to this Privacy Policy on our Services. We encourage you to revisit this policy regularly to stay informed about how we collect, use, and share your information.

12. Contacting us

If you have questions or concerns about this Privacy Policy or the use or disclosure of your information as described in this Privacy Policy, please contact us through support in the SOTG App or at support@surveysonthego.net (<mailto:support@surveysonthego.net>).





Phone

(714) 754-1234 (tel:+17147541234)

Why MFour

Validated Consumers

[\(https://mfour.com/validated-consumers/\)](https://mfour.com/validated-consumers/)

Validated Surveys

[\(https://mfour.com/vsurveys/\)](https://mfour.com/vsurveys/)

OmniTraffic® Behavior Data

[\(https://mfour.com/omnitraffic-data/\)](https://mfour.com/omnitraffic-data/)

Studio Data Platform

[\(https://mfour.com/mfour-studio/studio-overview/\)](https://mfour.com/mfour-studio/studio-overview/)

Products

Standard vSurveys

[\(https://mfour.com/standard-vsurveys/\)](https://mfour.com/standard-vsurveys/)

vSurveys+™

[\(https://mfour.com/vsurveys/\)](https://mfour.com/vsurveys/)

vTracker+™

[\(https://mfour.com/vtracker/\)](https://mfour.com/vtracker/)

OmniTraffic® Data

[\(https://mfour.com/omnitraffic-data/\)](https://mfour.com/omnitraffic-data/)



Blogs

(<https://mfour.com/resources/blogs/>)

Reports

(<https://mfour.com/resources/reports/>)

Use Cases

(<https://mfour.com/use-cases/>)

Top Findings

(<https://mfour.com/resources/top-findings/>)

Guides

(<https://mfour.com/resources/guides/>)

Insights Gallery

(<https://mfour.com/insights-gallery/>)

Careers

(<https://mfour.com/careers/>)



[Contact Us \(https://mfour.com/contact-us/\)](https://mfour.com/contact-us/)

[🐦\(https://twitter.com/mfourmobile\)](https://twitter.com/mfourmobile) [🎥\(https://vimeo.com/mfourmarketing\)](https://vimeo.com/mfourmarketing)

[in\(https://www.linkedin.com/company/mfour-mobile-research/\)](https://www.linkedin.com/company/mfour-mobile-research/)

[@\(https://www.instagram.com/mfourstudio/\)](https://www.instagram.com/mfourstudio/)

© 2024 MFour Mobile Research. All Rights Reserved.

[Privacy Policy](https://mfour.com/privacy-policy-2/) [Do Not Sell My Info](https://mfour.com/do-not-sell-my-info/)
[Subscribe](#) [\(https://mfour.com/privacy-policy-2/\)](https://mfour.com/privacy-policy-2/) [\(https://mfour.com/do-not-sell-my-info/\)](https://mfour.com/do-not-sell-my-info/)
[Terms of Use](https://mfour.com/terms-of-use/)
[\(https://mfour.com/terms-of-use/\)](https://mfour.com/terms-of-use/)