

Privacy Policy

Effective October 31, 2024

We recognize the importance of privacy and are committed to protecting the personal data of our customers and prospective customers, as well as other users of our websites, products and services (collectively referred to as the “Services”). This privacy policy (“Policy”) explains how Perceptyx, Inc. and our subsidiaries and affiliates (“Perceptyx”, “we”, “our”) handle the personal data that we collect and process about customers, prospective customers and users of our Services, as well as other individuals who otherwise engage or communicate with us about our Services.

California Consumer Privacy Act (“CCPA”). If you are a California resident, please review Section 13, *Additional Information for California Residents*, below, for important information about how we collect, use and disclose personal data about California residents and your rights under the CCPA.

Table of Contents

1. Scope
2. Personal data we collect
3. Purposes and legal bases of use
4. Disclosures of Personal Data
5. Cookies
6. How long does Perceptyx store your personal data?
7. How do we secure your personal data?
8. Your choices and rights.
9. International Transfers
10. Children
11. Contact Us
12. Additional Information for Individuals in Certain Jurisdictions
13. Additional Information for California Residents

1. Scope

This Policy applies to the personal data that we collect and process on our own behalf, as a “controller” or a “business” under applicable privacy laws and as a “processor” of the Customer Personal Data (as defined below) collected from our customers, as more fully explained below.

Personal data. In this Policy, our use of the term “personal data” includes other similar terms under applicable privacy laws—such as “personal information” and “personally identifiable information.” In general, personal data includes any information that identifies, relates to, describes, or is reasonably capable of being associated, or reasonably linked or linkable with a particular individual.

Customer Personal Data. Perceptyx contracts with companies to provide a variety of Services, including employee surveys and related services. When Perceptyx provides our Services to such a customer, we collect and process personal data of that customer’s employees on behalf of that customer. We refer to this data as “Customer Personal Data.” We are a “processor” or “service provider” with respect to our collection and processing of Customer Personal Data and will only process such Customer Personal Data on behalf of that particular customer in compliance with the applicable agreements, respectively, that we entered into with that customer. If you are an employee of one of our customers, this Policy applies to you to the extent your personal data is included in the Customer Personal Data, and your employer’s respective privacy policy also applies to and governs the processing of Customer Personal Data.

Controller and responsible party. For the purposes of the EU General Data Protection Regulation (the “GDPR”) and other relevant applicable laws (such as the UK Data Protection Act 2018 (“UK DPA”) and the Brazilian General Data Protection Law (the “LGPD”)), Perceptyx, Inc. is the “controller” of your personal data collected directly from you, for example, via our websites. With respect to any Customer Personal Data, our customers are the data “controllers” or “businesses” for their respective Customer Personal Data, and we are a “processor” or “service provider” as defined under applicable privacy laws.

2. Personal data we collect

We may collect personal data about you directly, as well as automatically related to the use of our websites and other Services or from third parties. The personal data that we collect and process, varies depending on the Services you use and your interactions with us. For example, you do not have to provide us with your personal data to access most of our websites but do need to provide us with certain personal data to use our other Services. However, if you choose not to provide certain information, you may be unable to access certain areas, or use our Services, and we may be unable to fully respond to your inquiries.

Information we collect directly. We may collect personal data about you directly from you or from your company. For example, when you fill out a “Contact Us” form, signup for our mailing lists, register for events we host or sponsor, or otherwise provide us information through our websites, we may collect personal data such as:

- Name, company name, and title/position
- Job title, other company information (such as country and industry sector)

- Business affiliations
- Email address, phone number, mailing address and contact details
- Contact preferences and interests
- Customer (and authorized user) account information (to access various parts of the platform Services), such as name, email address, telephone number, company name, and other information necessary to confirm that you are an authorized user of a customer
- Other information related to your request or inquiry
- Content you provide when participating in blogs, discussions, web forums, or similar interactive parts of our Services (the “Community”), including associated metadata

Automatically collected information. We use cookies, log files, pixel tags, local storage objects, and other tracking technologies to automatically collect information when users access or use the Services or visit our websites, such as IP address, general location information, domain name, page views, a date/time stamp, browser type, device type, device ID, Internet service provider, referring/exit URLs, operating system, language, clickstream data, and other information about the links clicked, features used, size of files uploaded, streamed or deleted, and similar device and usage information. For more information, see the Cookies and Similar Devices section below.

Information collected from third parties. We may collect personal data about you from third party sources, such as business partners, social media platforms, public sources, joint marketing partners (so that we can market and deliver our Services) and third parties to whom you have expressed interest in our Services, as well as information that you shared on social media platforms (subject to the respective platform terms and applicable laws).

3. Purposes and legal bases of use

In this section, we explain the purposes for which we process your personal data, as well as the legal bases for doing so under certain applicable laws.

Legal bases. Certain laws, including the GDPR, require that we inform you of the legal bases for our processing of your personal data. Pursuant to these laws, we process personal data for the following legal bases:

- Performance of contract: as necessary to enter into or carry out the performance of our contract with you or our customers.
- Compliance with laws: for compliance with legal obligations and/or defense against legal claims, including those in the area of labor and employment law, social security, and data protection, tax, and corporate compliance laws.
- Our legitimate interests: in furtherance of our legitimate business interests, which are not overridden by your interests and fundamental rights, including:
 - Performance of contracts with customers and other parties

- Implementation and operation of global support (e.g., IT) services for our business operations
- Improving our websites, developing trend and benchmark reports, and similar purposes
- Customer relationship management and improving our websites and Services, including other forms of marketing and analytics
- Fraud detection and prevention, including misuse of Services or money laundering
- Physical, IT, and network perimeter security
- Internal investigations
- Mergers, acquisitions, and reorganization, and other business transactions
- With your consent: where we have your consent, the GDPR (where it applies) and other applicable laws give you the right to withdraw your consent, which you can do this at any time by contacting us using the details at the end of this Policy. In some jurisdictions, your use of the Services may be taken as implied consent to the collection and processing of personal data as outlined in this Policy and your employer's privacy policy if they are a customer using our Services. In addition, we may process your personal data where necessary to protect the vital interests of any individual.

Purposes for which we collect and process your personal data. The purposes for which we may process personal data vary depending upon the circumstances. Generally, we use personal data for the business and commercial purposes listed below:

- Operating our websites and Services and providing related support: to provide and operate the Services, communicate with you about your use of the Services, provide troubleshooting and technical support, respond to your inquiries, fulfill your orders and requests, process your payments, communicate with you, and for similar service and support purposes. *(Legal bases: performance of our contract with you or our customers; and/or our legitimate interests)*
- Responding to requests: to respond to your inquiries and requests. *(Legal basis: performance of our contract with you or our customers)*
- Analyzing and improving the our websites, our Services, and our business: to better understand how users access and use the Services, in order to administer, monitor, and improve our Services, for our internal purposes, and for other research and analytical purposes. *(Legal basis: our legitimate interests)*
- Personalizing experiences: to tailor content we may send or display on our websites, including to offer location customization and personalized help and instructions, and to otherwise personalize your experiences. *(Legal basis: our legitimate interests)*
- Advertising and marketing to customers: to promote Perceptyx's Services on third-party websites, as well as for direct marketing purposes, including to send you newsletters, customer alerts and information we think may interest you. *(Legal bases: our legitimate interests; and/or with your consent)*
- Protecting our legal rights and preventing misuse: to protect the Services and our business operations; to prevent, detect and investigate fraud, misuse, harassment or other types of unlawful activities; where we believe necessary to investigate, prevent or take action regarding illegal activities, suspected fraud, situations involving potential threats to the safety or legal rights of any person or third party, or violations

of this Policy and our applicable agreements and terms of use. *(Legal bases: our legitimate interests; and/or compliance with laws)*

- Complying with legal obligations: to comply with the law or legal proceedings. For example, we may disclose information in response to subpoenas, court order, and other lawful requests by regulators and law enforcement, including responding to national security or law enforcement disclosure requirements. *(Legal bases: our legitimate interests; and/or compliance with laws)*
- Related to our general business operations: to consider and implement mergers, acquisitions, reorganizations, and other business transactions, and where necessary to the administration of our general business, accounting, recordkeeping and legal functions. *(Legal bases: our legitimate interests; and/or compliance with laws)*

Aggregate and anonymous data. We also create and use aggregate, anonymous and de-identified data to derive benchmark information which is made available to our customers, and to improve and develop our business and Services, and for similar research and analytics purposes.

Customer Personal Data. Our customers, not Perceptyx, determine the purpose and means of processing for their respective Customer Personal Data, including personal data collected and processed related to launching, analyzing and reporting on surveys and other products offered as part of the Services. In general, (subject to applicable customer instructions) Perceptyx processes the Customer Personal Data to provide our Services to customers, including to operate and improve Services generally, to provision Services user accounts, to carry out and to respond to user requests, to launch and track surveys, polls and other Services content. Our customers are the data controllers with respect to their Customer Personal Data. Please review the customer's respective privacy policies for more information about how they collect, use and share the personal data they collect.

4. Disclosures of Personal Data

In general, we may disclose personal data as explained below:

- Subsidiaries: to our subsidiaries, whose handling of your personal data is subject to this Policy. A list of our subsidiaries is available [here](#).
- Users: if you use, access or communicate with us about our Services on behalf of your company (our customer), we may share personal data about your access, and your communications or requests, with your company.
- Service providers: to third party service providers who perform functions on our behalf. Third party service providers will only process your personal data in accordance with our instructions and will implement adequate security measures to protect your personal data.
- Advertising and analytics partners: to third parties we engage to provide advertising, campaign measurement, online and mobile analytics, and related services to us (with your consent, where required by applicable laws)
- In response to legal process: in order to comply with the law, judicial proceedings, a court order, or other legal process, such as in response to a subpoena.

- **To protect our rights:** where we believe it is necessary to investigate, prevent or take action regarding illegal activities, suspected fraud, situations involving potential threats to the safety of any person, violations of the terms governing the use of the Services or this Policy, to respond to claims asserted against us or, or as evidence in litigation in which we are involved.
- **Business transfers:** as part of any merger, sale, and transfer of our assets, acquisition or restructuring of all or part of our business, bankruptcy, or similar event, including related to due diligence conducted prior to such event where permitted by law.

Aggregate or anonymous data. We may share aggregate, anonymous or de-identified data with third parties for research, analytics and other purposes, provided such information does not identify a particular individual.

5. Cookies

We and our third-party service providers who help us operate our websites use “cookies,” pixels, java script, log files, and other mechanisms to operate our website and to provide the Services.

Cookies. A “cookie” is a small text file that may be used, for example, to collect information about website activity. Some cookies allow us to make it easier for you to navigate our websites and platform, while others are used to enable a faster log-in process or to allow us to track your activities while using our websites or platform. For example, our websites use functional, analytical and tracking cookies to optimize the visitor experience. We use cookies to remember your IP-address, settings and preferences. In addition, we use other cookies, including those from third-party providers, to offer and improve our websites and Services to you, to make our websites user-friendly, and to personalize content and advertisements. Most browsers allow you to control cookies, including whether or not to accept them, and how to remove them. Click [here](#) to see the current list of cookies we use.

Clear GIFs, pixel tags and other technologies. Clear GIFs are tiny graphics with a unique identifier, similar in function to cookies. In contrast to cookies, which are stored on your computer’s hard drive, clear GIFs are embedded invisibly on web pages. We may use clear GIFs (also referred to as web beacons, web bugs or pixel tags) in connection with our Services to, among other things, track the activities users of our Services, help us manage content, and compile statistics about usage of our Services. We and our third-party service providers also use clear GIFs in HTML emails to our customers and users, to help us track email response rates, identify when our emails are viewed, and track whether our emails are forwarded.

Log files. Most browsers collect certain information, such as your IP address, device type, screen resolution, operating system version, and internet browser type and version. This information is gathered automatically and stored in log files.

Third-party analytics. We also use automated devices and applications, such as Google Analytics to evaluate use of our websites and collect usage statistics. These analytics providers may use cookies and other technologies to perform their services.

Do-not-track signals. Our websites do not respond to do-not-track signals. You may, however, disable certain tracking as outlined above (e.g., by disabling cookies). You may also use our preference manager to manage your cookie preferences on our websites.

Services platform. Our Services platform uses necessary and functional cookies to enable individuals to participate in surveys, to create or review surveys, and use our other products. For example, we use cookies to ensure a respondent can only take a survey once or come back to the survey if the respondent leaves the page in the middle of the survey.

6. How long does Perceptyx store your personal data?

As a general rule, we retain your personal data for as long as necessary to fulfill the purposes for which it was collected or as necessary to comply with our legal obligations, resolve disputes, maintain appropriate business records, and enforce our agreements. We may retain personal data for longer where required by our regulatory obligations, professional indemnity obligations, or where we believe we need to retain personal data to establish, defend, or protect our legal rights and interests or those of others. Our customers instruct us on how long to retain Customer Personal Data, which we handle as a data processor.

7. How do we secure your personal data?

We have implemented technical and organizational measures designed to protect your personal data against accidental or unlawful processing. For example, your personal data is encrypted while in transit and at rest. Regardless of the precautions taken by us, we cannot ensure or warrant the security of any information you transmit to us. Further, you are responsible for all actions taken with your user ID and password, if any. Therefore, we recommend that you do not disclose your user ID or password to anyone.

8. Your choices and rights.

If you wish to access personal data that you have submitted to us, to request the correction of any inaccurate information you have submitted to us, or to request deletion of your information, please send your request to remove@perceptyx.com. We will review your request and make reasonable efforts to respond to it as soon as practicable. We may ask you for additional information so that we can confirm your identity. If you would like to submit a request relating to Customer Personal Data, you should contact the relevant customer directly (most likely your employer); if you submit a request to us related to Customer Personal Data, we will forward your request to the relevant customer (where known), so that they may respond to your request.

Direct marketing. You may always opt-out of direct marketing emails. If you would like to unsubscribe from Perceptyx email subscriptions or otherwise change your email preferences with Perceptyx, please click [here](#) or follow the instructions in any Perceptyx promotional email that we send to you. We may continue to send you transactional or service-related communications, such as service announcements and administrative messages.

Complaints. We will take steps to try to resolve any complaint you raise regarding our treatment of your personal data. You also have the right to raise a complaint with the privacy regulator in your jurisdiction.

Additional Information for Certain Jurisdictions. In the section *Additional Information for Individuals in Certain Jurisdictions* below, we provide additional information as required under California privacy laws, as well as the GDPR, UK DPA and the LGPD. Users in California, the EEA, the UK, and Brazil should review this section for more information regarding their rights under these respective laws.

To submit a privacy request or exercise your rights regarding your personal data, please submit your request using our [Request Form](#) or send an email to privacy@perceptyx.com. We will respond to your request consistent with applicable law.

9. International Transfers

Perceptyx is a global operating organization with headquarters in the United States, and are subject to the investigatory and enforcement powers of the Federal Trade Commission (FTC). We have operations, entities and service providers in the United States, European Union and throughout the world. As such, we and our service providers may transfer your personal data to, or access it in, jurisdictions (including the United States, European Union, the United Kingdom and other jurisdictions where we, our affiliates and service providers have operations) that do not include equivalent levels of data protection as your home jurisdiction. We will take steps to ensure that your personal data receives an adequate level of protection in the jurisdictions in which we process it, including through appropriate written data processing terms and/or data transfer agreements. In the context of an onward transfer, Perceptyx has responsibility for the processing of Personal Data it receives under the EU-U.S. DPF and subsequently transfers to a third party acting as an agent on its behalf.

EU-U.S. Data Privacy Framework. Perceptyx complies with the EU-U.S. Data Privacy Framework (“EU-U.S. DPF”), the UK Extension to the EU-U.S. DPF (the “UK DPF Extension”), and the Swiss-U.S. Data Privacy Framework (“Swiss-U.S. DPF”) as set forth by the U.S. Department of Commerce. Perceptyx 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 and the United Kingdom in reliance on the EU-U.S. DPF and the UK DPF Extension. Perceptyx 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 (the EU-U.S. DPF Principles and the Swiss-U.S. DPF Principles are collectively referred to as the “DPF Principles”). If there is any conflict between the terms in this Policy and the DPF Principles, the applicable DPF Principles shall govern. To learn more about the Data Privacy Framework program, and to view our certification, please visit <https://www.dataprivacyframework.gov/list>. In compliance with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF, Perceptyx commits 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) and the Swiss Federal Data Protection and Information Commissioner (FDPIC) with regard to unresolved complaints concerning our handling of human resources data received in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF in the context of the employment relationship.

Under the Data Privacy Framework program, we have chosen the EU data protection authorities as the independent recourse mechanism to resolve complaints associated with the data you provide. In addition, you may also have the right to invoke binding arbitration as set forth in Annex I of the DPF Principles, provided that you invoke binding arbitration by delivering notice to your organization and following the procedures and subject to conditions set forth in Annex I of the DPF Principles.

Users in the European Economic Area (EEA) and United Kingdom. If you are in the EEA or the United Kingdom and we process your personal data in a jurisdiction that the European Commission has deemed to not provide an adequate level of data protection not covered by the EU-U.S. DPF, the UK DPF Extension, or the Swiss-U.S. DPF (a “third country”), we will implement measures to adequately protect your personal data, including by putting in place standard contractual clauses as approved by the European Commission (the form for the standard contractual clauses can be found at https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en). To obtain additional details of the mechanism under which your personal data is transferred outside of the EEA; you may request such details by contacting us as set forth in the Contact Us section below.

10. Children

We do not knowingly or specifically collect information about minors under the age of 16. If you believe we have unintentionally collected such information, please notify us as set out in the Contact Us section below.

11. Contact Us

If you have any questions or comments about this Policy, the ways in which we collect and use your personal data, your choices and rights regarding such use, or wish to exercise your rights, please do not hesitate to submit your request using our [Request Form](#) or contact us at privacy@perceptyx.com.

12. Additional Information for Individuals in Certain Jurisdictions

EEA (GDPR), UK and Brazil. Subject to the conditions set out in the applicable law, users in in the European Union/European Economic Area, United Kingdom and Brazil (as well as in other jurisdictions where similar rights apply) have the following rights regarding our processing of their personal data:

- **Right of access:** If you ask us, we will confirm whether we are processing your personal data and, if necessary, provide you with a copy of that personal data (along with certain other details).

- Right to correction (rectification): If the personal data we hold about you is inaccurate or incomplete, you are entitled to request to have it corrected. If you are entitled to have information corrected and if we have shared your personal data with others, we will let them know about the rectification where possible.
- Right to erasure: You can ask us to delete your personal data in some circumstances, such as where we no longer need it or if you withdraw your consent (where applicable). If you request that we delete your personal data, we may do so by deleting your account(s) with us. Brazilian Users may also request the anonymization, blocking or erasure of unnecessary or excessive personal data.
- Right to restrict (block) processing: You can ask us to restrict the processing of your personal data in certain circumstances, such as where you contest the accuracy of that personal data or you object to our use or stated legal basis.
- Right to data portability: You have the right, in certain circumstances, to receive a copy of personal data we have obtained from you in a structured, commonly used and machine readable format, and to reuse it elsewhere or to ask us to transfer this to a third party of your choice.
- Right to object: Where our processing is on the basis of our legitimate interests (other than marketing purposes), we must stop such processing unless we have compelling legitimate grounds that override your interest or where we need to process it for the establishment, exercise or defense of legal claims. Where we are relying on our legitimate interests, we believe that we have a compelling interest in such processing, but we will individually review each request and related circumstances.
- Right to object to marketing: You can ask us to stop processing your personal data to the extent we do so on the basis of our legitimate interests for marketing purposes. If you do so, we will stop such processing for our marketing purposes.
- Right not to be subject to automated decision-making: You have the right not to be subject to a decision when it is based on automatic processing if it produces a legal effect or similarly significantly affects you, unless it is necessary for entering into or performing a contract between us. Perceptyx does not engage in automated decision-making.
- Right to withdraw your consent: In the event your personal data is processed on the basis of your consent, you have the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal. Brazilian Users also have the right to be informed about the consequences of denying or withdrawing consent.
- Right to lodge a complaint: You also have the right to lodge a complaint with a supervisory authority if you consider that our processing of your personal data infringes the law.

Please note that some of these rights may be limited, such as where we have an overriding interest or legal obligation to continue to process the data. Please contact us using the information set out in the Contact Us section above, if you wish to exercise any of your rights or if you have any enquiries or complaints regarding our processing of your personal data.

We do not knowingly or specifically collect information about minors under the age of 16. If you believe we have unintentionally collected such information, please notify us as set out in the Contact Us section below.

13. Additional Information for California Residents

In this section, we provide additional information to California residents about how we handle their personal information, as required under California privacy laws including the California Consumer Privacy Act (“**CCPA**”). This section does not address or apply to our handling of publicly available information lawfully made available by state or federal government records or other personal information that is exempt under the CCPA.

While our collection, use and disclosure of personal information varies based upon our relationship and interactions with you, in this section we describe, generally, how we have collected and disclosed personal information about consumers in the prior 12 months.

Categories of Personal Information Collected and Disclosed. The table below identifies the categories of personal information (as defined by the CCPA) we have collected about consumers, as well as how we have disclosed such information for a business purpose. For more information about the business and commercial purposes for which we collect, use and disclose personal information, please see the Purposes and legal bases of use and Disclosures of personal information sections above.

Personal Information Collected		Categories of Third Parties to Whom We May Disclose this Information
Categories	Description	
Identifiers	Includes direct identifiers, such as name, alias user ID, username, account number; email address, phone number, address and other contact information; IP address and other online identifiers; SSN, driver’s license number, passport number, tax ID and other government identifiers; and other similar identifiers.	• service providers • advisors and agents • government entities and law enforcement • affiliates and subsidiaries • advertising networks • data analytics providers • social networks • internet service providers • operating systems and platforms • business customer/client

Customer Records	Includes personal information, such as name, account name, user ID, contact information, employment information, account number, and financial or payment information), that individuals provide us in order to purchase or obtain our products and services. [For example, this may include account registration information, or information collected when an individual purchases or orders our products and services, or enters into an agreement with us related to our products and services.	• service providers • advisors and agents • government entities and law enforcement • our affiliates and subsidiaries • business partners who provide services you request
Commercial Information	Includes records of personal property, products or services purchased, obtained, or considered, or other purchasing or use histories or tendencies.	• service providers • advisors and agents • government entities and law enforcement • affiliates and subsidiaries • advertising networks • data analytics providers • social networks • internet service providers • operating systems and platforms • data brokers • business customer/client

Usage Data	Includes browsing history, clickstream data, search history, access logs and other usage data and information regarding an individual's interaction with our websites, mobile apps [and other Services, and our marketing emails and online ads.	• service providers • advisors and agents • government entities and law enforcement • affiliates and subsidiaries • advertising networks • data analytics providers • social networks • internet service providers • operating systems and platforms
Audio, Video and Electronic Data	Includes audio, electronic, visual, thermal, olfactory, or similar information such as, thermal screenings and CCTV footage (e.g., collected from visitors to our offices/premises, photographs and images (e.g., that you provide us or post to your profile) and call recordings (e.g., of customer support calls).	• service providers • advisors and agents • government entities and law enforcement • affiliates and subsidiaries
Professional information	Includes professional and employment-related information such as business contact information and professional memberships.	• service providers • advisors and agents • government entities and law enforcement • affiliates and subsidiaries
Education Information	Information about an individual's educational history such as the schools attended, degrees you were awarded, and associated dates.	• service providers • advisors and agents • government entities and law enforcement • affiliates and subsidiaries

Inferences	Includes inferences drawn from other personal information that we collect to create a profile reflecting an individual's preferences, characteristics, predispositions, behavior, attitudes, intelligence, abilities or aptitudes. For example, we may analyze personal information in order to identify the offers and information that may be most relevant to customers, so that we can better reach them with relevant offers and ads.	• service providers • advisors and agents • government entities and law enforcement • our affiliates and subsidiaries • analytics providers
-------------------	--	---

Sources of Personal Information. We may collect personal information from the following sources:

- directly from the individual
- advertising networks
- data analytics providers
- social networks
- business customers

California residents' rights. In general, California residents have the following rights with respect to their personal information:

- Do-not-sell (opt-out): to opt-out of our sale of their personal information. We do not sell personal information about California consumers, including those we have actual knowledge are younger than 16.
- Right of deletion: to request deletion of their personal information that we have collected about them and to have such personal information deleted (without charge), subject to certain exceptions.
- Right to know: with respect to the personal information we have collected about them in the prior 12 months, to require that we disclose the following to them (up to twice per year and subject to certain exemptions):
 - categories of personal information collected;
 - categories of sources of personal information;
 - categories of personal information about them we have disclosed for a business purpose or sold;
 - categories of third parties to whom we have sold or disclosed for a business purpose their personal information;
 - the business or commercial purposes for collecting or selling their personal information; and
 - a copy of the specific pieces of personal information we have collected about them.

- Right to non-discrimination: the right not to be subject to discriminatory treatment for exercising their rights under the CCPA.

Submitting CCPA Requests. California residents may submit CCPA requests to know (access) and requests to delete their personal information by submitting requests using our [Request Form](#), or email at remove@perceptyx.com.

When you submit a request to know or a request to delete, we will take steps to verify your request by matching the information provided by you with the information we have in our records. You must email us with any requested information (or otherwise provide us with this information to verify your request. In some cases, we may request additional information in order to verify your request or where necessary to process your request. If we are unable to adequately verify a request, we will notify the requestor. Authorized agents may initiate a request on behalf of another individual by contacting us through the above listed method; authorized agents will be required to provide proof of their authorization and we may also require that the relevant consumer directly verify their identity and the authority of the authorized agent.

For more information about our privacy practices, you may contact us as set forth in the Contact Us section above.