

OUTLOGIC PRIVACY NOTICE

. *Please click [HERE](#) to opt-out of selling your data.

OUTLOGIC LLC a Virginia company (“OUTLOGIC” “we,” “us,” and “our”), provides data services to other companies and organizations, as further described in this privacy notice (“Privacy Notice.”).

This Privacy Notice explains how we collect, uses, stores, and shares personal information about individuals in two different contexts (we refer to such individuals as “you,” “your,” and “yourself”): (1) visitors to our website located at www.outlogic.io or (2) when we collect personal information from third parties such as mobile applications (“Apps”). t This Privacy Notice also explains certain choices you may have regarding how we use this information about you, as well as rights you may have to access or correct the information we hold and use.

If you are located in the European Economic Area (EEA) and would like to review your rights under the GDPR, please go to [Section 8](#) of this Privacy Notice. If you are a resident of California or Virginia or certain other states that have enacted privacy-specific consumer laws, you may review your data privacy rights under those types of state laws at [Section 10](#) of this Privacy Notice.

Please note that we do not use any precise location data to create or build consumer profiles or targeted audiences in connection with sensitive health based locations, nor do we permit our customers to do so. In addition, to further comply with specific state laws, we use commercially available information to assist in filtering out precise location data for sensitive health based locations in those states.

Below, we explain certain terms that we will use in this Privacy Notice that may make it easier to understand:

- *Advertising ID*: A unique alphanumeric string randomly assigned by operating system manufacturers to a Device. Examples of this include iOS IDFA's and Android Advertising IDs.
- *Data Aggregators*: Third party data companies that provide data to Outlogic, including personal data and information.
- *Devices*: Internet-connected mobile devices such as Apple iPhones that use iOS or Samsung Galaxy devices that use Google's Android OS.
- *IP Address*: a numeric address in a format that follows the Internet Protocol data rules and that is used to identify a computer, mobile phone, or other device connected to the internet.
- *Personal Information*: This Policy refers to "Personal Information" and "Personal Data" interchangeably, to mean the types of information/data that applicable laws that use those terms refer to. It includes, for instance, device identifiers, precise location data, name/address, email address, and other unique identifiers that can be associated with them.
- *Publishers: Providers of Apps used by Users on Devices*.
- *SDK, or Software Development Kit*: An SDK is a block of computer code that Publishers can integrate with their Apps to collect data, often useful (as in OUTLOGIC's case) to the mobile advertising and data industries.
- *Services*: OUTLOGIC's Services refer to the products and insights we create/provide using location data, and using and providing IP Addresses and/or Advertising IDs assigned by Device manufacturers, to companies for marketing and research purposes, for example, to enable their research and personalized advertising. The Services also refer to products and insights we provide using location data and/or Installation IDs assigned to Devices by certain Apps, to companies for research purposes, excluding marketing and personalized advertising. The Services also include the SDK and other similar technologies we may use to collect information.
- *Site*: Our website that you may visit at <http://www.outlogic.io/>.
- *Visitors*: Individuals who visit our website or choose to provide information directly to us via the OUTLOGIC website "Contact Us" form.
- *Server to Server App / Server to Server Partner*: OUTLOGIC sometimes partners with certain Publishers or other Data Aggregators, who (in each case) do not use the SDK in favor of sending us information they collect from their Apps using their own SDKs. In other cases, we may obtain the same kinds of information using server-to-server transfers instead of collecting information through SDKs.

- *System Location Services*: Device technologies that allow Apps to access information about your location (such as GPS coordinates).
- *Installation ID*: A unique alphanumeric string randomly assigned by certain Apps to a Device but which is not used for advertising purposes.
- *App Tracking Transparency/Opt-Out of Interest Based Ads*: Features on iOS or Android Devices that allow Users to disable, or limit Apps' ability to access, the Device Advertising ID. On iOS phones, users who do not give Apps permission to track zeroes out the Advertising ID. On Android phones running Android 12 or newer, users whom Opt-Out of Interest Based Ads zeroes out the Advertising ID.

A. Summary: Who is OUTLOGIC?

OUTLOGIC is a platform for collecting, aggregating, licensing and managing data. In particular, we focus on the curation and use of high-quality location data to help provide insights to organizations of various kinds regarding patterns of peoples' movements. Our platform assists a variety of businesses and organizations in understanding movement patterns and trends for purposes including marketing and advertising, financial research, market research, traffic and urban planning, smart cities, or educational purposes. Certain government entities or public health organizations may also use our platform, including for purposes of public health research and planning, information security, physical security, to prevent crime, or for civic and traffic planning. (Our specific data licensing practices may vary depending on geographic region).

2. What Types of Information Do We Collect?

A. Information We Collect Through Our Services

We collect information using our SDK. This information may include Advertising IDs, Installation IDs, location information (described more fully below), and other information pertaining to the way Devices and their users engage with mobile advertising services. We also collect the same types of information using Server to Server transfers. We also collect information (including location information) from Publishers to assist them in meeting revenue goals for their Apps, allowing them to provide media, games, and other mobile apps, such as weather or traffic

apps, without charging their users. We also may collect and use information from Apps owned by OUTLOGIC affiliated companies.

Publishers can use our SDK with their Apps in order to enhance advertisers' ability to show ads in Publisher Apps (including to target more relevant ads and to measure ad performance). App Publishers may also work with us to monetize their App content in other ways we describe in this Privacy Policy. (If you would like to opt-out of our use of the Advertising ID on your Device for these purposes, please take the steps explained in [Section 6](#) below, entitled "User Choices and Opt-Out Tools").

When you use an App or OUTLOGIC App on your Device that has integrated with our Services (including the SDK), we can collect certain information through or about your Device, if you have granted access to (and you have not later opted-out of our use of) location services and an Advertising ID or Installation ID. In particular (but not exclusively):

- a. Precise Location Information:
 - Specific geolocation of the Device, usually described by latitude-longitude coordinates compiled through GPS features of our SDK, Wi-Fi connection information, cell tower triangulation and other methods.
 - Dwell time within or in proximity to points of interest (i.e. the length of time your device stayed at one place).
- b. Relative Location Information:
 - Bluetooth Low-Energy (BLE) sensors, or beacons,
 - Information obtained from the Internet of Things (IoT) devices.
 - Near-field Communication (NFC)
 - Our SDK is capable of receiving signals from each of the above technologies that indicate the proximity of a Device. For example, certain brick-and-mortar stores use beacons that sense when a Bluetooth-enabled Device is in proximity to the beacon (i.e., when a Device user enters the store). Retail locations, sports arenas, restaurants, museums and other similar businesses may also use beacons.
- c. Advertising IDs or Installation IDs
- d. Timestamps (that may include time and date)
- e. Device Event Information:

- App or system crashes
- System crashes
- Device settings
- f. Device Usage Information
 - Type of device (e.g., Samsung Galaxy S21)
 - Operating system (OS) information (e.g., iOS 14.5)
 - System settings (e.g., enabled/disabled status for Location Services)
 - Time zone
 - Mobile carrier
 - IP address
 - Names and/or identifiers for Apps on your Device integrated with SDK
- g. Network Information
 - VPN status
 - Network protocols employed
 - Device connectivity information (e.g., how a device connects to a network) and signal strength
 - Network information such as mobile network code and mobile country code

B. Site Visitors

OUTLOGIC, along with our service providers and other vendors, collect information from visitors (“Visitors”) to our Site, including information Visitors choose to provide to us on contact forms or through our support email addresses, including support@outlogic.io, as well as information collected through passive, automated means such as cookies and web pixels, as follows:

- a. Information Visitors Choose to Share: We may collect your full name, physical address, telephone number, and email address if you provide it to us. For example, you may choose to give us this information to register for an event, to learn more about our Services, or to set up an account with our platform. Our platform users may give us additional information, such as employer or payment information. You may learn more about our use of this type of information by emailing privacy@outlogic.io.
- b. Information about Browsers or Devices: We may collect information about your computer (e.g. desktop or laptop), Device, tablet, or other internet-

connected devices used to access the Site. This information may include technical details about your computer or Device (such as the Device type, operating system, system settings and configurations, IP address, Advertising ID or other unique Device-based IDs, and mobile network carrier information) and information about how you use the Site (including details about the parts of the Site you access, traffic to and from other websites, timestamps, web log data, and other event information, including crashes and system activity). You may exercise control over this type of data collection by adjusting the settings on your device or browser (e.g., by disallowing cookies and using other similar settings).

- c. Cookies: We, along with our service providers and other vendors, may place cookies on our Visitors' web browsers. You may view our full cookie policy [here](#). We may use cookies for retargeting and other types of interest-based advertising, which you may limit by exercising the opt-out choices described in [Section 6](#).
- d. Web Beacons: Web beacons or "pixels" are small, invisible webpage or email elements that may be used on the Site or in emails we send to you. We use them to deliver cookies, to count Site visits, to understand Site usage, to study the effectiveness of our advertising or marketing offers, and to learn whether you open an email or act upon it. You may limit this type of re-targeting and other types of interest-based advertising by exercising the opt-out choices explained in [Section 6](#).

3. How We Use The Information We Collect Through Our Services

When we collect information through the Services, OUTLOGIC [or its customers who receive the data](#) may use it for any of the following purposes:

- a. To Make Inferences based on collected data, including movement patterns and research:
 - *Movement Patterns*: To make inferences regarding the location and movement patterns of individuals or devices. For example, we might record location data from Devices at certain points of interest over time, like shows, sporting events, restaurants, etc., and we may include this information in the Services.
 - *Data Products*: To use these location-based observations with other data products. For example, we may add other information to the

location data we collect such as the name of a venue, time spent at a point of interest, or other information to a set of Advertising IDs or Installation IDs to enhance user profiles or to enable decision-making based on that information, such as executing a stock trade.

- *Advertising and Research*: For advertising and research purposes, such as use by advertising technology platforms who use the information to provide similar capabilities. The information helps these platforms to make predictions and generate insights about trends in consumer or market behavior, or to conduct scientific research in connection with human movement patterns.
- *Smart Cities and Security*: Real estate developers, urban planners, government entities, or security or smart city businesses may use and augment the information to tailor it to their needs. We also license the information to assist businesses and governments with planning, physical security, information security, and preventing crime.

b. Interest-Based Audiences and Targeting Ads:

- *Interest-Based Audiences*: We use the information we collect to organize Device users into audience segments based on their inferred interests (for example, that a Device user is interested in attending sporting events, or certain kinds of retail stores). This enables our Clients to deliver advertising to those users when they are recognized on their own platforms.
- *Targeting Ads*: By using audience segments, advertisers increase their chances of sending an ad that is more likely to be relevant.

c. Ad Measurement:

- *Ad Measurement Analysis*: We use information we collect (such as location information and Advertising IDs) to assist advertisers with analyzing ad campaign performance – for example, by measuring how (or whether) Devices that were served with a particular ad engaged with the advertiser's products or services. This is sometimes called ad measurement or attribution analysis.
- An example of ad measurement analysis would be if certain Devices were served with an advertisement for "OUTLOGIC Sandwich Shop" on Wednesday, and location data then showed traffic at OUTLOGIC Sandwich Shop on Thursday or Friday was higher than average,

OUTLOGIC Sandwich Shop might conclude that its ad campaign performed well.

d. Publisher Analysis:

- *Analysis and Compliance:* We assist our Publisher partners with analyzing how Users engage with the Publishers' Apps, and in activating that information for advertising, to generate revenue, and to enhance App functionality.
- We may also use this information to provide Publishers with options for complying with certain laws, regulations, and other rules where applicable.

To learn more about how we share information, please refer to [Section 5](#).

4. How Do We Use Information We Collect From Visitors?

We may use information we collect about Visitors for our corporate and internal purposes, including:

- a. Analyzing what products and services Visitors may be interested in, the popularity of different pages of our Site, as well as how Visitors interact with our Site in other ways. If you give your personal contact information to us (e.g., your email address), we may combine that information with other information described in [Section 2](#) to understand how to better serve you.
- b. To communicate with Visitors, including to offer customer or Visitor support for the Site or the Services. For example, we may use your personal information solely for purposes of replying to your questions when you use the "Contact Us" form on the Site or send us an email at support@outlogic.io.
- c. Market research.
- d. Direct and online targeted marketing in accordance with applicable law. For instance, we may "retarget" ads about our services to those who have visited our website.
- e. To improve, maintain, operate, and personalize the Site.
- f. For human resource purposes.
- g. For any other legitimate purpose upon proper notice and/or consent.

5. With Whom Do We Share Information We Collect?

We share the information we collect for purposes of operating our platform (for example, with our service providers) and for purposes of supporting the business of our customers. We may share information we collect from your Device as follows:

a. With Our Customers:

- We share Advertising IDs, Installation IDs, Location Information, App Usage Data, and audience segments generated from those data points, with our customers ("Clients").
- Our Clients may include brand advertisers, data and technology platforms, advertising technology companies, and other organizations that study consumer behavior, provide tailored advertising, or study human movement patterns.
- Like OUTLOGIC, some of these Clients may be members of the Network Advertising Initiative ("NAI"). To learn more about the NAI and your opt-out options that the NAI offers (and requires its members to provide), please see <https://www.networkadvertising.org/choices/>. OUTLOGIC is not responsible for these Clients' or any third parties' privacy policies or opt-out programs or their compliance with NAI requirements.

b. With Our Service Providers:

- We have contracts with businesses that assist us with our own business operations (e.g., our Site, database hosting, fraud detection and prevention, verification and reporting, data hygiene, human resources, marketing and advertising, and email services), as well as billing or accounting functions, collections, technology, and other forms of operational support.

c. With Our Affiliates:

- In the event we establish a subsidiary or otherwise become affiliated with another company, we may share any information that we have collected with those entities.

d. In Relation to Legal Proceedings or Process:

- We may share information we have collected when we have a legal obligation to do so. This may include compliance with a binding court

- order, exercising, establishing or defending OUTLOGIC's legal rights, or those of Clients or any other third party, or in good faith to comply with the requirements of any applicable law or legal process.
- Similarly, we may disclose any information we have collected as required to respond in good faith to legal process, including subpoenas (whether civil or criminal), court orders or search warrants.
- e. To Investigate Malfeasance and to Defend or Protect Ourselves or Third Parties:
- We may share information to assist us in enforcing our legal rights, our Terms of Service, or other policies as applicable, or to investigate any potential violation of the same. We may also share information to investigate any potential violations of the law, to defend or protect ourselves, our Clients, or any third party from any potential harm (whether tangible or intangible).
- f. In Relation to a Corporate Transaction:
- If a third party seeks to acquire or actually acquires our business or assets in whole or in part, we may disclose information we have collected in connection to that transaction (including without limitation during due diligence that may be undertaken in advance of possible sales).

6. User Choices & Opt-Out Tools

You can manage the way that we use data collected passively from your Device in connection with the OUTLOGIC Site and the Services (e.g. Advertising IDs, Installation IDs, or cookies) as described below:

- a. Browser Settings: You may adjust the privacy and security settings of your web browser to change how your browser uses cookies.
- b. Opting Out of Interest Based Advertising on Mobile Devices: You can opt out of tailored advertising on mobile devices by companies that participate in the Network Advertising Initiative or the Digital Advertising Alliance by visiting the NAI's Mobile Choices Page and following the instructions provided there.
- c. You can opt out of interest-based advertising on your browser by participating companies by visiting the [NAI's opt-out page](#) or the [DAA's](#)

Consumer Choice Page. Residents of the EEA, UK and Switzerland may refer to www.youronlinechoices.com. The opt-out tools provided on these industry pages are generally based on cookie technologies. As such, if you delete your cookies (or change or update your web browser) you will need to repeat the opt out process. While our Services are generally not based on cookie technology, we are providing this information because we may partner with businesses to tailor ads for our own Services that do (for example, to retarget Visitors of Sites with advertisements). Further, certain third-party platforms may use information we have collected to match identifiers across devices – such as to tie a mobile Advertising ID by common IP Address to a browser-based cookie ID.

- d. OUTLOGIC Opt-out: You may limit the ways we use certain information we have collected by submitting an opt-out request by visiting this link: *Your Privacy Choices and Opt-Out Rights*. [here](#).
- e. Our Marketing Emails: If you receive marketing or promotional emails from us, you may opt out of receiving those messages by following the “unsubscribe” instructions contained in them, or by emailing us with your request at privacy@outlogic.io. If you opt out of our marketing and promotional messages, you may still receive transaction- or service-related emails about your business relationship with us.

7. Security

We use administrative, technical, and physical safeguards designed to protect our physical infrastructure as well as in our computer systems, databases, and communications networks. These measures are intended to protect our systems (and the information contained therein) from loss, misappropriation, misuse, alteration or disclosure. No method of electronic transmission or storage is perfectly secure, however, so we cannot guarantee the security of information we collect with absolute certainty.

8. The European Union and UK and Protections Under European Privacy Laws (GDPR and UK GDPR)

We (and those using our Services) are required to provide certain information about the processing of “Personal Data” of users in EEA and Switzerland under the GDPR of users in the UK under the UK GDPR. For purposes of this explanation, we will refer to both as “GDPR.” “Personal Data” generally refers to data that identifies or is capable of identifying a particular user or Device. Names and addresses, cookie IDs, Advertising IDs, Installation IDs, precise location information, and biometric data are examples of “Personal Data.”

If you have any questions about OUTLOGIC’s processing of Personal Data in the context of the GDPR, You may contact our Chief Privacy Officer by emailing your questions to privacy@outlogic.io, or contact our EU Representative at eurep@outlogic.io.

The representations and information we provide below, which are applicable only to individuals located in the EEA, the UK and Switzerland, are provided for purposes of compliance with the GDPR. Please do not rely on the information below if you are not located in one of those regions.

- a. Legal grounds for processing your Personal Data: Under the GDPR, we must disclose the legal bases we rely on to process Personal Data. Our legal bases for processing Personal Data for the purposes we describe in [Section 2](#) and [Section 3](#) above and [Section 5](#) as to our corporate data) include:
 - *Consent.* We rely on your consent to provide our Services that use precise location information related to other Personal Data. We also rely on your consent to store and access information on your Device (e.g., Advertising IDs and Installation IDs). Our reliance on consent is in turn often in reliance on compliance steps required of and taken by our data suppliers and by Clients that use the Services. These steps are intended to confirm that your consent is collected in compliance with the GDPR and passed on to Clients and business partners such that we only facilitate the collection of data in compliance with the law. We may rely on your consent to process Personal Data in other circumstances as well. When we do so, we will follow applicable laws pertaining to providing and withdrawing consent. We also attempt to obtain consent for certain of our clients to process Personal Data. These Clients, in turn, may be

independent data controllers as to data in their own possession and control.

- *Legitimate interest.* We may rely on legitimate interest as a legal basis for processing Personal Data in some cases. We may do so when we use Personal Data for purposes of maintaining the security of our services (including to detect and prevent fraud or to facilitate the detection and correction of bugs or other errors). We also rely on legitimate interest when we use our own Clients' Personal Data (or our Site Visitors' Personal Data) to communicate with them about their use of our Services, or to analyze user activity on our Site.
 - *Contractual Agreements.* In some cases our basis for processing Personal Data is that the processing is necessary pursuant to a contractual relationship we have entered into (such as records and contact information related to our Clients). You may obtain a copy of our SCCs document by contacting us at privacy@outlogic.io.
 - *Legal Obligations.* We may process Personal Data when it is necessary for us to comply with our legal or regulatory obligations.
- b. Transfers of Personal Data: When we collect Personal Data in the EEA, UK, or Switzerland, and then transfer it outside of those jurisdictions, we take measures to ensure that such Personal Data is protected by appropriate safeguards. In general, our transfers of Personal Data rely on Standard Contractual Clauses and Data Processing Agreements to safeguard that data where the GDPR or other European data protection laws require it. You may use the contact information below to request a copy of these SCCs..
- *How We Retain Personal Data:* We generally retain Personal Data we collect for as long as is necessary to either (1) provide our Services (absent a deletion or opt-out request); or (2) for other purposes including compliance with our legal obligations, dispute resolution, and to enforce our contracts. Our schedule for retaining Advertising IDs, Installation IDs, and related location data is as follows: Advertising IDs and Installation IDs we collect in order to provide our Services are rendered inactive by us within 12 months after the time we last obtained your consent; however, we may retain data beyond 13 months where we have de-identified it (i.e., altered it in such a way that it cannot be linked to Personal Data). We may retain this (and other) information insofar as we have a legal or

operational need to do so, for example, for purposes of auditing, corporate record-keeping, legal compliance, accounting, security and bug-prevention purposes.

- c. **Rights of Data Subjects:** Data Subjects have certain rights in connection with the Personal Data that data controllers process about them pursuant to the GDPR. These include the right to access Personal Data, the right to request correction of inaccurate Personal Data, the right to request the restriction of processing of Personal Data, the right to request deletion of Personal Data, and the right to object to processing of Personal Data (including when we process Personal Data to build a profile for targeted digital advertising). We describe these rights more fully below.

- ***Right to Access:*** You may contact us at privacy@outlogic.io in order to exercise your right to access Personal Data we process as a data controller. We will respond to your request by explaining the steps you must follow to access your Personal Data after we receive your request. Because we are required to verify the identity of the individual making a request before we provide access to Personal Data, we will evaluate requests to exercise certain rights to access Personal Data on a case-by-case basis. In conducting this evaluation, we may consider both (1) the effort involved in verifying whether Personal Data that we process actually pertains to the data subject making the request – and only to that data subject; and (2) any potentially negative consequences that may result from erroneously releasing Personal Data to an individual other than the data subject, in light of the sensitivity of the Personal Data at issue and the degree of certainty we can achieve through verification. We may also limit the amount or kind of Personal Data we will release in circumstances where we believe it is likely that the improper release of Personal Data would adversely affect the privacy rights and freedoms of the data subject. We will only honor requests for access to Personal Data for which we act as a data controller, as explained more fully in sub-section (d) below. Where we act as a processor for Personal Data on behalf of another entity (for example, our Clients), you may contact that company instead of OUTLOGIC to make a data access request.
- ***Right to Correct:*** You may exercise your right to correct Personal Data by contacting us using the contact information provided below.

- *Right to Withdraw your Consent or Object to our Personal Data Processing:* You may use the opt-out methods described in [Section 6](#) of this Privacy Notice to withdraw your consent for our processing of your Personal Data (when we are relying on your consent). If you withdraw your consent, we will stop processing your Personal Data in connection with our Services within 30 days or fewer.
 - *Right to Request Deletion:* You have the right to request that we delete Personal Data concerning you that we process as a controller. If you use the opt-out process described above, we will also delete your Personal Data. You may also contact us at privacy@outlogic.io to request that we delete your Personal Data. We will provide further instructions on how you can exercise your right to deletion after we receive your email request. In certain circumstances we may keep copies of Personal Data in back-up files (or otherwise in inactive form), for certain of our internal purposes that are important to our business, including legal, auditing, accounting and billing, bug-detection and correction. We may keep such backups for as long as is necessary to fulfill those purposes.
 - *Right to Make Complaints:* You have the right to lodge a complaint regarding our processing of Personal Data with a relevant data protection authority. If you have a complaint, please contact us first to allow us to assist you in resolving it.
- d. OUTLOGIC may act as either a data controller or a data processor in connection with the Personal Data we process, depending on the circumstances. EU data protection law distinguishes between companies that process Personal Data for their own purposes (i.e. “data controllers”) and companies that process Personal Data on behalf of and at the direction of other organizations (i.e. “data processors”). When we act as a data processor for other organizations, such as for our Clients, we may direct your requests or inquiries to the relevant data controller that is responsible for the processing of your Personal Data.

9. Children’s Data

We do not intend for our Services to be used in connection with minors under the age of 18, and we do not intentionally collect data from them. If you believe that

we may have inadvertently collected of any such data, please use the contact information provided in [Section 12](#) below to let us know.

10. Additional Information for U.S. Residents Including Residents of California, Colorado, Montana, Connecticut, Utah, Virginia and other States with Applicable Privacy Rights

US residents have data deletion rights as described in this Section 10. In addition, California residents have certain privacy rights under the California Consumer Privacy Act of 2018 as amended by the California Privacy Rights Act of 2020 (“CCPA”), and Virginia residents have similar privacy rights under the Virginia Consumer Data Protection Act of 2019 (“VCDPA”), with respect to personal information or personal data about them. Residents of Colorado, Connecticut and Utah have similar rights under either the Colorado Privacy Act (“CPA” effective July 1, 2023), the [Connecticut Act Concerning Personal Data Privacy and Online Monitoring](#) (“CTDPA” effective July 1, 2023), or the [Utah Consumer Privacy Act](#) (“UCPA” effective December 31, 2023). A number of other states’ residents have or will have similar protections at various times beginning in 2024 and 2025. We refer in this section to all states with privacy laws relevant to the below rights and disclosures as “Applicable States”).

A useful guidemap to consult as to what privacy laws exist in your state is located at <http://iapp.org/resources/article/us-state-privacy-legislation-tracker/>. (we are not responsible for the content in that tracker, which is not ours but rather is provided by a third party organization.)

Under the CCPA “Personal Information” generally means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Similarly, under the VCDPA and other state privacy laws, “Personal Data” means any information that is linked or reasonably linkable to an identified or identifiable natural person. When we use the term “personal information” in the following sections, we mean your personal data or information under the CCPA if you are a California resident or your Personal Data under the laws of other Applicable States.

If you are a resident of the US including any of the Applicable States, this section of the Privacy Notice applies to you insofar as we have collected personal information about you, or have sold such information.

As required by the CCPA and VCDPA, and the other Applicable States laws when they become effective, we describe the personal information we collect about residents of US states, and the purposes for which we may use it, in the following sections:

- A. Categories of Personal Information We Collect; How We Use It; and How We Share with Third Parties
- B. The Business Purposes We Have for Collecting and Sharing Personal Information
- C. Rights and Choices of US States Residents
- D. Retention of U.S. Personal Information

A. Categories of Personal Information We Collect; How We Use It; and How We Share with Third Parties

We may collect the categories of personal information about you described in the table below, depending on how you interact with us or our Services. The table also describes the categories of third-parties with whom we may share the categories of personal information specified. You may exercise your Right to Access in connection with any of the Personal Information Categories in the table below.

PERSONAL INFORMATION CATEGORY	DO WE CURRENTLY COLLECT/USE THIS CATEGORY OF PERSONAL INFORMATION?	SOURCES WE COLLECT THIS CATEGORY FROM:	HAVE WE "SOLD" THIS CATEGORY OF PERSONAL INFORMATION IN THE PAST 12 MONTHS?	CATEGORIES OF THIRD PARTIES WHOM THIS DATA WAS SHARED WITH FOR BUSINESS PURPOSES
-------------------------------	--	--	---	--

Identifiers (e.g., online identifiers; IP address; mobile ad identifiers, other online or advertising platform identifiers)	Yes	Data analytics services and data aggregators; Third party mobile applications and websites; and OUTLOGIC affiliate owned and operated mobile applications and websites	Yes	Advertising networks (e.g., demand-side platforms, agency trading platforms); Agencies and advertisers; Data aggregators and resellers; Data analytics services; Financial institutions; Government entities and information services; Outlogic affiliates; and App Publishers
Identifiers related to our own corporate “business to business” purposes and/or our Site (these are not utilized with our Services to Clients, but instead for, e.g., our own	Yes	Data analytics services and data aggregators; Third party mobile applications and websites; and OUTLOGIC	No	Operating systems and platforms

marketing and
Approved Partner
contact purposes):
name, address, e-
mail address,
phone number

affiliate
owned and
operated
mobile
applications
and websites

Internet or Other Yes
Electronic Network
Activity Information
(e.g., information
regarding a
consumer or
device's interaction
with a website or
application)

Data Yes
analytics
services,
data
aggregators,
and
OUTLOGIC
affiliate
owned and
operated
mobile
applications
and websites

Advertising
networks (e.g.,
demand-side
platforms, agency
trading
platforms);
Agencies and
advertisers; Data
aggregators and
resellers; Data
analytics
services;
Financial
institutions;
Government
entities and
information
services; Outlogic
affiliates; and App
Publishers

Geolocation
Information
(lat/long
coordinates,
generally
associated with a
mobile identifier)

Data Yes
aggregators;
Third party
mobile
applications;
and
OUTLOGIC
affiliate
owned and

Advertising
networks (e.g.,
demand-side
platforms, agency
trading
platforms);
Agencies and
advertisers; Data
aggregators and

operated
mobile
applications

resellers; Data
analytics
services;
Financial
institutions;
Government
entities and
information
services; Outlogic
affiliates, and App
Publishers

Data analytics Yes
services
and data
aggregators;
Third party mobile
applications and
websites;
and OUTLOGIC
affiliate owned and
operated mobile
applications
and websites

Inferences (for example, whether a consumer is likely to be interested in travel, or sports events, or another activity)

Advertising networks (e.g., demand-side platforms, agency trading platforms); Agencies and advertisers; Data aggregators and resellers; Data analytics services; Financial institutions; Government entities and information services; Outlogic affiliates; and App Publishers

B. The Business Purposes We Have for Collecting and Sharing Personal Information

Our purposes for collecting and sharing Personal Information are described below (with examples). These details are also described in our Privacy Notice:

- Tailored Digital Advertising:
 - a. Working with advertisers, agencies and the technology platforms they use to: (1) target (such as by creating inferred audience groups), send, tailor, optimize and analyze advertising and marketing messages in websites, mobile apps or across other channels; and (2) measure and analyze the effectiveness of those messages.
 - b. Create “identity” graphs to assist our Clients in finding users across multiple channels. This may include linking personal, device-based, or network-based identifiers (e.g., Advertising ID, Installation IDs, or IP address).
- Research for Marketing and Other Purposes:
 - a. We provide information for purposes including financial and market research, for the study movement patterns, for urban planning, for

smart cities research, or for educational purposes. We may also share information with government entities or public health organizations who wish to study movement patterns for disease prevention research, for physical security or defense purposes or information security, to prevent crime, or for civic, disaster and traffic planning.

- To Operate Our Services: We use personal information to:
 - a. Enhance, test, update, and verify our own data and data-related services
 - b. Develop new products or services
 - c. Operate, analyze, enhance, and secure our services
- Other Internal Business Purposes:
 - a. We use personal information for internal research or operations, auditing, detecting and responding to security incidents, debugging, short-term and transient use, quality control, and legal compliance. Information we collect from our Sites and from Apps may be used for the above, in addition to our own marketing purposes.
 - b. *Sharing for Purposes of Legal Compliance:* We may share personal information with third parties for purposes of: (1) compliance with official legal process or a regulatory investigation (for example, a valid subpoena or court order); (2) enforcing our Terms of Service, this Privacy Notice, or other agreements, including investigation of suspected violations of the same; (3) responding to claims that certain content violates the rights of third parties; or (4) protecting the rights, property or personal safety of us (or our platform), our Clients, our affiliates, our agents, our platform users, or the general public. Similarly, we may share personal information with other entities to detect or prevent fraud, to prevent spam or malware, or other similar purposes.
 - c. *Sharing In Connection With a Corporate Transaction:* In the event of a major corporate transaction (such as a merger, investment, acquisition, reorganization, consolidation, bankruptcy, liquidation, or sale of some or all of our assets), we may share personal information in connection with that transaction, including for purposes of associated due diligence.
 - d. *Sharing With Our Service Providers:* We may share any personal information we collect with our service providers. Our service

providers may include, for example, providers of: technology; support for our Clients; business operations; web or database hosting; billing; accounting; physical or information security; marketing and advertising; data management, validation, enhancement or hygiene; or providers that otherwise assist us with providing, developing, maintaining, or improving our Services.

- e. *Aggregate Information:* We may use personal information to create aggregate information, or may de-identify any personal information we collect to make it such that it cannot be linked to you or your device (“Aggregate or De-Identified Information”). We may use Aggregate or De-Identified Information for any purpose, including, but not limited to, for research and marketing purposes. We may also share Aggregate or De-Identified Information with third parties, who may include advertisers or marketers, promotional partners, our sponsors, or otherwise at our discretion.

C. Rights and Choices of US States Residents

If you are a resident of any US state, you have the right to request that we delete personal information collected from you, including data that may reveal your mobile device’s precise geographic location, and also send requests to any recipients of your personal information that they delete such data from their commercial databases (your “deletion rights”). If you choose to exercise your right to deletion, there are certain circumstances under which we may nevertheless retain personal information as permitted by law, such as to prevent, detect, or investigate data security incidents, or to protect against malicious, deceptive, fraudulent, or illegal activity directed at the company. The right to delete is separate from the right to opt-out of data sales as provided in Applicable States laws. We describe below how you may exercise your deletion rights.

In addition to data deletion, if you are a resident of an Applicable State, you may have additional rights including the right to request (1) that we disclose what personal information we collect from you; and (2) to opt out of our sale of your personal information. The states that provide these rights to their residents include but are not limited to California (under the CCPA), Colorado (under the CPA), Connecticut (under the CTDPA), Utah (under the UCPA), and Virginia (under the VCDPA), as well as other Applicable States, as we have stated above. These rights are subject to certain limitations, although you will not be

discriminated against for exercising any of these rights. In certain circumstances, we may charge a reasonable fee to process your request to the extent permitted by law.

a. Right to Opt-out of the Sale of Your Personal Information:

- Residents of Applicable States may opt out of the “sale” of their personal information. “Sale” is defined broadly by various state laws, to include making personal information available in exchange for any monetary or other valuable consideration. ”
- To “opt out” of our “sale” of your personal information you may use either of the methods below:
 - a. By visiting this link: *Your Privacy Choices and Opt-Out Rights*.
 - b. by emailing your opt-out request to privacy@outlogic.io using a subject line that reads “Data Transfer Opt out.”

b. Right to Request Deletion of Your Personal Information:

- If we have collected personal information from you, you may request that we delete such personal information. A request to delete is distinct from a request to “opt out” of our sale of your personal information. You may contact us by email at privacy@outlogic.io or call us toll-free at +1 866-346-9602 to exercise this right.
- If you choose to exercise your right to deletion, there are certain circumstances under which we may nevertheless retain personal information as permitted by law, such as:
 - a. To defend against fraudulent activity directed towards our business, systems, or users.
 - b. To detect and fix technical issues that affect existing system functions (e.g., for de-bugging).
 - c. As necessary for the protection of the free speech or other rights of us (or others).
 - d. To assist with law enforcement requests made pursuant to lawful process.
 - e. For certain scientific or historical research purposes.
 - f. For our own internal purposes, provided they are reasonably related to your relationship with us.
 - g. To comply with our legal obligations.

- Please note that we require certain information in order to provide our Services to you. If you ask us to delete that information, it may prevent you from being able to access or use our Services.
- [Opt-Out/Access/Deletion Request Metrics-2024](#)
From January 1, 2024, to December 31, 2024, we maintained processes to facilitate requests pursuant to the California Consumer Privacy Act. We received the following requests, and responded as follows:

a. As to requests to know:

We received 10

We complied with 2

We denied 8, as the limited personal data collected is logged by a device ID. The requestor refused to provide the necessary device ID despite the company's follow up explanation and request.

Our median response time was 2 days. Our mean response time was 3 days.

b. As to requests to delete:

We received 141

We complied with 8

We denied 133, as the limited personal data collected is logged by a device ID. The requestor refused to provide the necessary device ID despite the company's follow up explanation and request.

Our median response time was 2 days. Our mean response time was 3 days.

c. As to requests to opt out of sale:

We received 543

We complied with 94

We denied 449, as the limited personal data collected is logged by a device ID. The requestor refused to provide the necessary device ID despite the company's follow up explanation and request.

Our median response time was 2 days. Our mean response time was 3 days.

d) We received an additional 24,800 requests by a purported third-party automated data deletion service. Such requests could not be processed, due to service's failure to provide the necessary identifying information despite our repeated requests.

c. Right to Request Access to Your Personal Information:

- Applicable States may give their residents the right to request that we disclose both the categories and specific pieces of personal information that we collect, use, or sell. We will comply with data access requests if we can verify them to a legally sufficient degree. You may make such an access request by emailing us at privacy@outlogic.io with the subject line “Data Access Request” or by calling us toll-free at +1 866-346-9602 .
- We may be able to adequately verify access requests for certain information we have collected. However, in line with certain guidance provided by the California Attorney General, we do not provide location data in response to access requests due to the fact that we are not able to verify to a reasonably high degree of certainty that the location data we have collected pertains to the individual making such a request, or whether either an individual with custody of a device — or the person making the request — is the rightful owner of the device to which the information we hold pertains. For example, it is not uncommon for a person to be in possession of another person’s phone temporarily (for example, a partner, friend or work colleague’s mobile phone or tablet), whether or not such temporary possession is authorized. We take this approach in order to avoid a scenario where such a person in temporary possession of a phone might obtain potentially detailed and sensitive information pertaining to the phone’s owner through a request for access. We also believe California law compels us to avoid a scenario like this. In addition, a recent study found that roughly 50% of mobile phones were not password protected at all, making the possibility of such “spoofing” a tangible risk. Further, we do not have other, more conventional means to confirm the identity of a device’s true owner because for consumer privacy reasons we do not collect information such as name, address or email address that could be used to do so.
- If you do not wish location data associated with your device to be used in the ways we describe above, we suggest that you make a request to opt out of sales of your information as detailed above. You can find complete information about how to exercise your right to opt out by visiting this link: *Your Privacy Choices and Opt-Out Rights*.

d. Our Collection of Sensitive Personal Information, and Your Rights to Limit Its Use:

- Certain Personal Information that we collect and sell, such as precise geolocation of a person, household, or device, is considered “Sensitive Personal Information” under the data privacy laws of California (CCPA), Connecticut (CTDPA), and Virginia (VCDPA) and other Applicable States. We obtain the right to use and share this information, through the consent methods described in our Privacy Policy. California residents have the right to require a business to limit the use of their Sensitive Personal Information to only certain internal business purposes specified in the CCPA.
- To limit the use of your Sensitive Personal Information, you may use either of the methods below:
 - a. By visiting this link: *Your Privacy Choices and Opt-Out Rights*.
 - b. By emailing your request to privacy@outlogic.io using a subject line that reads “California Limit SPI Use.”

e. How to Exercise Your Rights and Submit a Verifiable Consumer Request:

- To exercise applicable privacy rights or to learn more about how to do so, residents of those Applicable States may contact us using any of the following means:
 - a. By visiting this link: *Your Privacy Choices and Opt-Out Rights*.
 - b. By emailing your request to privacy@outlogic.io.
 - c. With respect to access or deletion requests, by calling us toll free at: +1 866-346-9602 .
- In certain circumstances, we may not disclose some personal information to you in response to an access request where doing so presents too great a risk to you or our business. We may also withhold such information where we cannot verify your identity in connection to such personal information.
- To learn about how to opt out of Tailored Advertising, please review and consider whether to use the industry opt-out mechanisms provided on the [NAI \(Network Advertising Initiative\) page](#). We believe that opting out using these industry tools may be more efficient, faster, and more uniform compared to using manual opt out processes.

- In the event we are not able to comply with your requests fully for any of the reasons described above, we will still explain the reasons why we could not fulfill your request. Certain consumers have the right to appeal our decision not to fulfill a request, and may do so by emailing our Chief Privacy Officer at Appeals@outlogic.io with the subject line “Privacy Choices Appeal.”
- f. Right to Non-Discrimination:
 - If you elect to exercise your A rights under the Applicable State, as described in this Section 10, we will not deny, charge different prices for, or provide a different level of quality of goods or services for that reason.
- g. Information Regarding Individuals Younger than 16 Years Old:
 - Unless we have obtained legally sufficient consent to do so, we do not knowingly sell personal information pertaining to minors younger than 16 years old. In the event we learn that we have collected or sold personal information regarding such residents, we will take reasonable steps to remove such information from our database (or we will obtain any legally required consents).
- h. Authorized Agents:
 - You may exercise your rights described above under the laws of Applicable States , by designating an agent to make requests on your behalf. If you choose to designate an agent, we will take steps to verify both (1) your identity; and (2) that your designated agent has been authorized to make a request on your behalf by providing us (depending on the legal requirement in your state) with a written authorization signed by you or a copy of a valid power of attorney.

D. Retention of U.S. Personal Information

We retain personal information pertaining to the categories listed in Section 10.A. on the following schedule: device and other identifiers, precise location data, inferences, and internet and other electronic activity information may be retained for up to 5 years, with certain aggregated information related to locations of devices and internal reporting data be retained for up to 3 years to fulfill the business purposes listed in Section II.B. We may maintain personal information for longer periods if we have a significant operational or legal need to do so, such as for auditing, compliance, accounting, security, bug-prevention purposes, and

when required by law. For example, we may retain Consent audit logs for up to 10 years.

11. Changes to This Privacy Notice

In the event we make material changes to this Privacy Notice that may affect you, we will post prominent notice of any such changes on our website for not less than 30 days prior to the effective date of the changes. If you wish to stay abreast of all such changes, we suggest that you check this Privacy Notice frequently in order to stay informed of any such changes.

12. Contact Information

To ask questions about the information in this Privacy Notice or for more information about how we use information we collect, or to exercise any of the rights outlined in Section 8 or Section 10, you may contact us at:

privacy@outlogic.io

OR

P.O. Box 17247
Arlington, VA 22216

OR

For EEA Residents: Please contact our EU Representative at eurep@outlogic.io Alternatively, they can be reached by post (The DPO Centre, Alexandra House, 3 Ballsbridge Park, Dublin, D04C 7H2) or +353 1 631 9460. <https://www.dpocentre.com/contact-us/>

For UK Residents Please contact our UK Representative at ukrep@outlogic.io Alternatively, they can be reached by post (The DPO Centre Ltd, 50 Liverpool street, London, EC2M 7PY) or +44 (0) 203 797 6340. <https://www.dpocentre.com/contact-us/>

Last Update: January 2025