

OUTBRAIN USERS PRIVACY POLICY

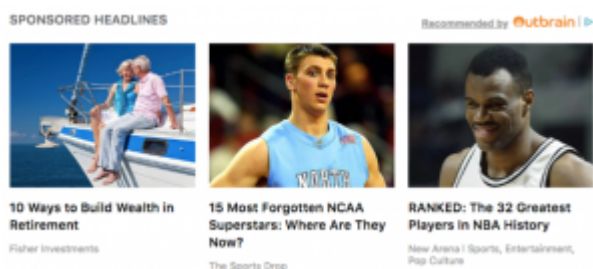
Last Updated January 2025

Outbrain is committed to protecting your Personal Data. For purposes of this Privacy Policy, “**Personal Data**” means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with you.

We use your Personal Data in line with all applicable laws. To ensure compliance and to align with Outbrain’s values around trust and transparency we have a team of privacy champions responsible for continuously implementing our global privacy program. Citizens from “European Territories” mean the European Economic Area (EEA), the European Free Trade Area (EFTA) and Switzerland.

This Users Privacy Policy (“**Users Privacy Policy**”) governs Outbrain’s use of User Personal Data. We may change this Users Privacy Policy from time to time. You are a User when you visit a page of a website or application of one of Outbrain’s partners (“**Partners**”) where the Outbrain widget is installed or our recommendations are placed (“**Partner Sites**”). For example, if you visit <https://news.sky.com/uk>, www.spiegel.de or www.cnn.com, the Outbrain widget is implemented on those websites. You know you are engaging with an Outbrain widget when you see the AdChoices logo directing you to Outbrain and/or text referencing Outbrain (e.g., “Recommended by Outbrain”, “by Outbrain”) near recommendations. If you click on the AdChoices logo you will see a detailed notice enables you to navigate to [Outbrain’s Interest Profile](#) and this Users Privacy Policy where you can opt out of personalized recommendations. In some instances, a Partner may have a white-labelled version of Outbrain’s service for their own offering. In such an event, such Partners must disclose their use of Outbrain in their privacy policies.

Example of an Outbrain Widget



For more information on how Outbrain uses your Personal Data when you visit www.outbrain.com (or any derivation/any of our other sites, such as Outbrain.co.uk; Outbrain.fr; outbrain.de, <https://www.zemanta.com/> etc.) (our “Sites”), please see [Outbrain’s Site Visitors Privacy Policy](#).

If you are a business partner of Outbrain and want to find out more information about how Outbrain uses personal data of its business partners, please see [Outbrain’s Business Partner Privacy Policy](#).

1. Who we are, what we do, how you can contact Outbrain, our DPO or the relevant authorities

a) Who we are:

This Privacy Policy applies to Outbrain Inc., a corporation registered in Delaware (USA) whose main office is in New York; and its affiliated subsidiaries (collectively, “Outbrain,” or “we”, “us”, “our”). We operate in various offices around the world and we partner with publishers and marketers across the globe.

If you are in the UK, or any European Territory, the controller of your data is Outbrain UK Limited. In general, our publishers and advertisers are joint controllers with us for the initial processing of your data when a publisher or advertiser client implements the Outbrain technology on their pages. For all subsequent processing by Outbrain, we are independent controllers with our publisher and advertiser clients. For a more detailed explanation of the roles and responsibilities of the parties, please see our publisher data sharing agreement [here](#) and advertiser data sharing agreement [here](#).

b) What we do:

Outbrain’s mission is to serve interesting recommendations to users when they visit a Partner site based on their interests. To achieve our mission, we enter into agreements with:

- online publishers and partners who want to recommend relevant content to their readers (this is [Outbrain Engage](#)); and
- advertising partners who want readers to view their content (this is [Outbrain Amplify](#)).

For further information on our Amplify (advertising partner) services see [here](#) and our Engage (media partners) services see [here](#). For further information on our Outbrain DSP services, please see [here](#).

c) How to contact us:

We regularly review our compliance with this Users Privacy Policy. Questions, comments and requests regarding this Users Privacy Policy are welcomed and should be addressed in the first instance to privacy@outbrain.com.

If Outbrain does not satisfactorily answer your questions or concerns, you may also contact the following for advice, support or complaints:

- Outbrain’s Data Protection Officer (“DPO”) at dpo@outbrain.com;
- the [Information Commissioner’s Office](#), which is Outbrain’s supervisory authority in the UK; and/or
- [Slovenia SA](#) which is Outbrain’s lead supervisory authority within the European Territories.

2. Alliances and adherence

- We adhere to the Self-Regulatory Principles set forth by the [Digital Advertising Alliance](#) (DAA) and the [European Interactive Digital Advertising Alliance](#) (EDAA);
- We are members in good standing of the [Network Advertising Initiative](#) (NAI), an association dedicated to responsible data collection and its use for digital advertising. We also adhere to the NAI Code of Conduct. Outbrain also adheres to the Interactive Advertising Bureau’s (IAB) Self-Regulatory Principles for Online Behavioral Advertising, and the IAB Europe TCF vendor ID; and
- We are also TAG Brand Safety Certified [here](#).





3. **What information we collect, how and why**

- a) We mainly process your Personal Data so that we can serve interesting recommendations. We may also process your Personal Data to create associated reports and to prevent fraud. Outbrain's recommendations may be paid for by an advertiser linking you to a new website or they may be organic such that the link is to another page on the same Partner's Site.
- b) We collect and process the following Personal Data in the following ways:

Generally, we use cookies, pixels and other similar technologies to collect and store Personal Data about you. In particular:

- **UUID (Unique User ID) and other online identifiers**

When you, as a User, first visit a Partner Site (e.g., CNN.com), Outbrain drops a cookie on your device in order to generate a UUID. Alternatively, if you first interact with a Partner using that Partner's application, Outbrain receives your advertiser ID which is assigned to you by your device. We catalogue and analyze the content you consume across Partner Sites. Our recommendations are based on: (i) a UUIDs browsing history; (ii) similar browsing patterns of other Users; (iii) recommendations that are generally popular with Outbrain's audience at this time; (iv) some randomness, and (v) targeting requirements that may be provided or requested by our Amplify clients. As an example, Outbrain may know that UUID 123 (which could be you on your iPhone X on The Guardian using Chrome as your browser) likes to read about far away holiday destinations and that people who like to read about far away holiday destinations also like to read about exotic food. When you interact with Outbrain we do not collect traditional Personal Data from you, like your email address or name, therefore we cannot associate your name with your UUID (for example, we do not know that John Smith, who is also UUID 123, likes to read about far away holiday destinations).

The UUID is a sequence of numbers and/or letters. This UUID attaches itself to your device and varies depending on your browser combination. In other words, Outbrain records a different UUID depending on which device and/or which browser you use when accessing the Partner Sites. For example, you will have one UUID when you visit a Partner Site from your mobile phone using the browser Safari, and a different UUID when you visit a Partner Site from your iPad using the browser Safari. Outbrain will combine and consolidate a UUID from a mobile device (handheld or tablet) from a browser that then accesses an application (or vice versa) from that same device. Outbrain does not conduct cross device tracking and therefore cannot link a user interacting with Outbrain on their phone as the same user who is interacting with Outbrain on their desktop.

We may also collect an Outbrain DSP (Formerly known as Zemanta) online identifier and advertiser ID which operate similarly to as described above. Please see the Outbrain DSP Privacy Policy [here](#) for more information.

- **IP Address**

In addition to your UUID, we recognize your IP address, which we translate into non-precise location data and delete the last octet in order to mask the identifying information. We use your IP address, in conjunction with information we received from other trusted third-party partners (such as MaxMind) to determine a broad understanding of where you are located (e.g., New York). Outbrain will still recognize your IP address even if you opt out of personalized tracking as this is necessary to continue serving you context-based recommendations; however, in such instances your IP address is not associated with your UUID and would not form part of any user profile.

- **Other Usage Information**

In addition to your UUID and IP address, we also collect the following information from you on:

- desktop and mobile web: (i) User Agent data: device type (e.g., iPhone), browser type (e.g., chrome), operating system (e.g. iOS); (ii) the pages visited; (iii) the time of visit; and (iv) referring URLs and other information normally transmitted in HTTP requests. The above statistical information provides us with information about how many Users

visited a specific page on our Partner Sites on which the Outbrain widget is installed, how long each User stayed on that page, the type of content on that page they clicked on and how they generally engaged with that page; and

- on applications: (i) application version (as it appears in App Store or Play Store); (ii) application ID or package name (as it appears in the App Store or Play Store); (iii) operating system (e.g. IOS or Android); (iv) operating system version; and (v) device model (e.g. iPhone X). This information is considered personal data if Outbrain associates it with a UUID.

We also use your Personal Data (individual profiles, preferences, characteristics, and behaviors) to make inferences and audience segments (some examples which can be found [here](#)).

c) Machine learning techniques

Outbrain uses non-generative machine learning techniques to process Users' Personal Data and to analyze trends and popular recommendations to predict what you will be interested in and what advertisement to show you based on this. Users will not be subject to decisions that will have a significant impact on them based on automated decision-making unless we have notified Users and have a lawful basis for doing so.

d) Legal basis for processing

As Outbrain does not control the Partner Sites upon which its technology is implemented, Outbrain relies on its partners to provide Users with relevant notices and consent management solutions. Where required by your applicable jurisdiction, we will only process your Personal Data where we have a legal basis to do so. The legal basis will depend on the purposes for which we have collected and use of your Personal Data. In almost every case the legal basis will be one of the following:

- **Consent:** For example, where you have provided your consent via a consent management platform.
- **Our legitimate business interests:** Where it is necessary for us to understand our customers, promote our services and operate effectively, provided in each case that this is done in a legitimate way which does not unduly affect your privacy and other rights. These legitimate interests include the operation of the Outbrain technology.
- **Compliance with law:** Where we are subject to a legal obligation and need to use your Personal Data in order to comply with that obligation.

4. How to manage the cookies and other similar technologies we use

a) Outbrain cookies

Please see the Users [Cookie Table](#) under for a detailed list of the cookies we use when you interact with Partner Sites where the Outbrain technology is implemented.

b) Outbrain pixels

In addition to Outbrain's visible widget on Partner Sites, certain Outbrain advertisers or publishers may implement the Outbrain pixel on their websites. The pixel can be used to create segments of users for retargeting purposes. The Outbrain pixel determines whether the User reaching the page where the pixel is installed has an Outbrain UUID in order to either provide attribution tracking to advertisers or publishers in respect of their particular campaign or to create audience segments for advertisers or publishers wishing to retarget relevant users for future campaigns. If there is a UUID associated with such end user, Outbrain allows advertisers to either retarget those UUIDs and/or provides advertisers with the total number of Users (on an aggregated and anonymized basis) that reached a particular page (for example, an advertiser does not know that UUID1234 converted but only that 1 conversion took place). Outbrain does not pass its advertisers any Personal Data (including your UUID) or collect any further Personal Data via the pixel.



c) Third party pixels

If you click on a link to one of our recommendations, the advertiser sponsoring the recommendation may place cookies (or third-party cookies of third parties acting on the advertiser's behalf) on your device either through redirects prior to arriving on the destination page of the recommendations or upon reaching the destination page. Such cookies are dropped for the purposes of providing analytics to the advertiser with regards to the advertiser's campaign (for example, to see how many users viewed the advertiser's campaign). We require our advertisers to disclose the use of third-party pixels and/or cookies to end users via their website. As these cookies and/or pixels are added at the sole discretion of our advertisers, you will be subject to that advertiser's privacy notice and/or privacy policy.

We also require our partners to disclose the usage of the Outbrain pixel on their own websites. Outbrain may also allow certain trusted third-party partners to collect data via cookies delivered through the Outbrain widget. In such cases, Outbrain does not pass these third parties the data which Outbrain collects on its Users but allows such third parties to directly collect data (including personal data) via the widget for fraud and/or security purposes or in order to provide measurement information to advertisers (such as the number of conversions and/or impressions). You can find a list of Outbrain's Trusted Partners [here](#).

d) Mobile advertising identifiers

Mobile advertising IDs (like IDFA) are unique IDs associated with individual mobile devices which Outbrain uses to associate with a user profile. Users can reset them by instructing their device to do so.

e) General web analytics

We may use web analytics from time to time, for example, our DSP service integrates with its client and partner's Web Analytics software in order to observe how users behave after clicking on ads. Any data collection via web analytics software is governed by such client's and/or third party's privacy policy.

5. Your rights

a) Outbrain opt out on desktop and mobile web

You may opt out of Outbrain's personalized recommendations (or, if you have opted out and would like to opt back in) at any time by moving the toggle below. You may also opt out of personalized recommendations via [Outbrain's Interest Profile](#) which is a website that allows you to exercise your data subject rights, including opting out of behavioral advertising, deleting your user profile or accessing the data Outbrain may hold on you.

b) Outbrain opt out on apps

In order to opt-out of Outbrain's recommendations on your mobile applications you can follow the steps below:

1. iOS Devices: Settings > Privacy > Advertising > Limit Ad Tracking
2. Android Devices: Google Settings App > Ads > Opt Out of Interest-based Advertising

Please note that an opt out via our Interest Profile and/or this Privacy Policy will not opt you out of personalized tracking on your applications. This opt out must be done via your device settings.

c) Additional opt-out options

You may also opt out of receiving personalized ads served by us or other advertising companies through industry powered tools such as the NAI or the various DAA-based pages ([DAA](#), [DAAC](#), and/or [EDAA](#)). Visiting the NAI, DAA, DAAC, or EDAA consumer choice pages allows you to opt out of all some or all of the participating members' services. Like Outbrain's opt out, these opt outs do not mean you will no longer receive any advertising, the advertisements will just not be tailored to you. You will continue to receive advertisements, for example, based on the particular website that you are viewing (i.e., [contextually based ads](#)). Also, if your browsers are configured to reject cookies



when you visit the DAA, DAAC or EDAA consumer choice pages, your opt out may not be effective as our opt out is cookie based.

If you are located in the European Territories/UK, please see Section 8 below which outlines other rights that you may exercise. If you are a resident of California or certain other states within the United States, please see Section 9 below which outlines other rights that you may exercise, depending on your state of residency.

IMPORTANT INFORMATION

Even though you have opted out of Outbrain's personalized recommendations:

- **You will still see Outbrain recommendations.** Opting out of Outbrain personalization tracking does not mean you will no longer receive recommendations from Outbrain. Instead, it means that Outbrain's recommendations will not be personalized (i.e. they will be context-based recommendations).
- **Your opt out will be cookie based and device/browser specific.** If you browse the web from several **devices** and/or browsers, you will need to opt out from each device and/or browser to ensure that we prevent personalization tracking on all of them. For the same reason, if you buy a new device, change browsers or delete (or clear) the opt out cookie, you will need to opt-out again. Opting out of personalization tracking is not the same as blocking cookies.
- **As with most opt out cookies, the Outbrain browser opt out relies upon a cookie.** The opt-out cookie is intended to be persistent to honor the user's preferences. However, the "Intelligent Tracking Prevention" feature in iOS11 may impact the persistence of cookies across websites post a 24 hour window. We suggest using another browser or considering blocking all 3rd party cookies from the browser so that you are "opted out" without needing to rely on any company's actual opt out methodology.
- **Your local storage will not be cleared.** Even though you have opted out of Outbrain's personalized recommendations your local storage will not be automatically cleared and therefore you need to clear this at a browser level in addition to your opt out.

6. Security Measures, Transfers Outside the EEA, Sharing and Data Retention

a) Security

Please see our [security standards](#) for more information on the security standards that Outbrain has in place.

Please remember that, unfortunately, the transmission of information via the internet is never completely secure. A common Internet scam is known as "spoofing" or "phishing." This occurs when you receive an email from what appears to be a legitimate source requesting Personal Data from you. Please be aware that we will not send you any emails requesting you to verify credit card, bank information, or any other Personal Data. If you ever receive an email that appears to be from us requesting such information from you, do not respond to it, and do not click on any links appearing in the email. Instead, please forward the email to us at legal@outbrain.com, as we will investigate instances of possible Internet fraud.

Our Sites contain links to other websites that we do not own or operate. We do not control, recommend or endorse the content, products, services, privacy policies or practices of these third party websites. If you choose to click on these links, you should know that these sites are not owned or operated by Outbrain and therefore these third party websites may send their own cookies to your device and they may independently collect personal data. It is therefore important that you get familiar with the privacy policies of these third party websites.

b) Sharing

Outbrain may share certain elements of a user profile (for example, UUID) with the following partners, including:

- Brand safety, analytics and fraud partners;
- Demand Side Platforms (DSP) and Supply Side Platforms (SSP);
- Ad Exchanges and/or Networks; and



- Demand Management Platforms.

Please see [here](#) for a list of our trusted partners (which may be updated from time to time). In addition, we may collect and/ or share some Personal Data with trusted partners by virtue of participating in the OpenRTB. Many of these partners are registered as IAB TCF Global Vendors and can be found [here](#). We may also allow third parties to collect data directly from you - please refer to our [Trusted Partners](#) and/or the Users section of our [Cookie Policy](#).

In addition, we may also disclose Personal Data as follows:

- within the family of companies controlled by Outbrain for internal reasons, primarily for business and operational purposes;
- if we go through a business transition, such as a merger, acquisition by another company, or sale of all or a portion of our assets, your Personal Data will likely be among the assets transferred;
- when legally required to do so (e.g., to cooperate with law enforcement investigations or other legal proceedings);
- to investigate reports of fraud or to protect against unauthorized use;
- to protect Outbrain's rights and property; and/or
- to respond to a genuine emergency.

We may also combine your Personal Data with that of other users in order to share trend information and aggregate user statistics with third parties, always in aggregated and anonymized form.

If you are a United States resident, please see Section 9 below for more information on how your Personal Data may be sold, "shared" and disclosed, as defined by the California Consumer Privacy Act and other state privacy laws.

c) **Data Retention**

The retention period for each of the cookies Outbrain uses (whether our own or on our behalf by third parties) is stated in the [Cookie Table](#).

More specifically, the Outbrain cookie (obuid), which is used for tracking user actions such as clicks, expires three (3) months after a User visited a particular site within our network; however, this cookie will reset if a User returns to the same site or different site within our network. In addition, we do not retain any individual data point on a User for more than 13 months. For example, if UUID 123 read an article on December 31, 2018, on February 1, 2019 that article will no longer be part of UUID 123's profile.

7. **Children and Sensitive Data**

None of our services are intentionally directed at children under 16 (or 13 if you are based in the US). We do not knowingly collect Personal Data from anyone under 16 years of age. If we determine upon collection that a User is under 16, we will not use or maintain their Personal Data. If we become aware that we have unknowingly collected Personal Data from a child under the age of 16, we will make reasonable efforts to delete such information from our records in accordance with applicable law. If you're a kid, please go play in the yard, don't use or interact with Outbrain!

8. **European Territory/UK Visitors**

a) **Your rights**

In compliance with certain privacy laws, in particular the European General Data Protection Regulation (GDPR) and the UK GDPR, you have certain rights in relation to your Personal Data. More specifically and under certain circumstances:

- the right to request information about whether and which Personal Data is processed by us, and the right to request that such Personal Data is rectified or amended;
- the right to request that your Personal Data be deleted;
- the right to request that the processing of your Personal Data be restricted or object to the



processing of your information on grounds relating to his or her particular situation, or at any time for direct marketing purposes;

- withdraw your consent to the processing and use of your data completely or partially at any time with future application;
- have the right to obtain your Personal Data in a common, structured and mechanically readable format, and to transmit those data to another controller;
- contact our data protection officer if there are any questions, comments, complaints or requests in connection with our statement on data protection and the processing of your Personal Data; and
- the right to complain to the responsible supervisory authority if believed that the processing of your Personal Data is in violation of the legislation.

We will handle any request to exercise your rights in accordance with applicable law and any relevant legal exemptions. If you wish to exercise any of these rights or have any questions, please email privacy@outbrain.com.

b) Data transfers outside the European Territories/UK to non-US territories

Our data centers are located in the US, Netherlands and Singapore. We transfer Personal Data from the European Economic Area (EEA) and/or UK to our data centers in the United States. When we transfer Personal Data, we will ensure such transfers are in compliance with relevant data protection laws, including, if applicable, EU/UK Standard Contractual Clauses, or a European Commission/UK Government positive adequacy decision.

In other words, your rights and protections remain with your data and we use approved contractual clauses and other measures designed to ensure that the recipients of your Personal Data protect it. Outbrain has in place the Standard Contractual Clauses between Outbrain entities to govern the transfer of data outside of the EEA/UK. To obtain more information as to the safeguards that we implement in this respect or to obtain a copy of them, please email privacy@outbrain.com.

For more detail on transfers to the United States, please see below.

c) Data transfers outside the European Territories/UK to US territories - EU-US Data Protection Framework (DPF) Participation

i. EU-US Data Protection Framework (DPF) Participation

Outbrain Inc. complies with the [EU-U.S. Data Privacy Framework \("EU-U.S. DPF"\)](#), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework ("Swiss-U.S. DPF") as set forth by the U.S. Department of Commerce. Outbrain has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) with regard to the processing of Personal Data received from the European Union in reliance on the EU-U.S. DPF and from the United Kingdom (and Gibraltar) in reliance on the UK Extension to the EU-U.S. DPF. Outbrain has certified to the U.S. Department of Commerce that it adheres to the Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) with regard to the processing of Personal Data received from Switzerland in reliance on the Swiss-U.S. DPF. If there is any conflict between the terms in this Privacy Policy and the EU-U.S. DPF Principles, the EU-U.S. DPF Principles shall govern. To learn more about the Data Privacy Framework (DPF) program, and to view our certification, please visit <https://www.dataprivacyframework.gov/>.

ii. Complaint and Dispute Resolution Procedure under the DPF

Outbrain's internal complaints mechanism

In compliance with the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF, Outbrain commits to resolve EU-U.S. DPF Principles-related complaints about our collection and use of your Personal Data. EU, UK and Swiss individuals with inquiries or complaints regarding our handling of Personal Data received in reliance on the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF should first contact Outbrain at:



DPO@outbrain.com

You may have the right to lodge a complaint with the data protection authority of your country of residence. If you live in the UK, you can make a complaint with the Information Commissioner's Office (ICO) [at this address](#). If you live in the EU, you can find the relevant data protection authority [here](#). To submit a complaint to the FTC, click [here](#).

Independent Recourse Mechanism

In compliance with the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF, Outbrain commits to cooperate and comply with the advice of the panel established by the EU data protection authorities (DPAs), the UK Information Commissioner's Office (ICO), the Gibraltar Regulatory Authority (GRA), and the Swiss Federal Data Protection and Information Commissioner (FDPIC) with regard to unresolved complaints concerning our handling of personal data received in reliance on the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF. The Federal Trade Commission has jurisdiction over Outbrain's compliance with the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF.

Arbitration

You may also be able to invoke binding arbitration for unresolved complaints but prior to initiating such arbitration, a resident of a European country (including Switzerland) participating in the DPF must first:

- (1) contact us and afford us the opportunity to resolve the issue;
- (2) seek assistance from [JAMS](#) (an independent recourse mechanism); and
- (3) contact the U.S. Department of Commerce (either directly or through a European Data Protection Authority) and afford the Department of Commerce time to attempt to resolve the issue.

If such a resident invokes binding arbitration, each party shall be responsible for its own attorney's fees. Please be advised that, pursuant to the DPF, the arbitrator(s) may only impose individual- specific, non-monetary, equitable relief necessary to remedy any violation of the DPF Principles with respect to the resident. The arbitration option may not be invoked if the individual's same claimed violation of the Principles has previously been subject to binding arbitration; was the subject of a final judgement entered in a court action to which the individual was a party; or was previously settled by the parties. For more details, please click [here](#).

iii. **OUTBRAIN'S LIABILITY IN CASES OF ONWARD TRANSFERS TO THIRD PARTIES**

In the context of an onward transfer, Outbrain has responsibility for the processing of Personal Data it receives under the DPF Principles and subsequently transfers to a third party acting as an agent on its behalf. Outbrain remains liable under the DPF Principles if its agent processes such Personal Data in a manner inconsistent with the DPF Principles, unless Outbrain proves that it is not responsible for the event giving rise to the damage.

9. **United States Consumer Privacy Notice**

This United States Consumer Privacy Notice ("State Notice") supplements the Outbrain Privacy Policy and provides additional information for residents of certain states with comprehensive privacy laws, such as California. This State Notice applies to Personal Data we collect, use and disclose from those applicable U.S. state residents.

a) **Your State privacy rights**

As a resident of certain U.S. states, you may have the right to submit certain requests relating to your Personal Data, as listed below, depending on your state of residency, such as California. However, these rights are not absolute, and in certain cases we may decline your request as permitted by law.



- **Right to Know.** If you are a California resident, you have the right to know what Personal Data we have collected about you, which includes:
 - The categories of Personal Data that we have collected about you.
 - The categories of sources from which the Personal Data was collected.
 - The business or commercial purpose for collecting, selling, sharing or disclosing the Personal Data.
 - The categories of Personal Data that we sold or shared, and for each category identified, the categories of third parties to which we sold or shared that Personal Data.
 - The categories of Personal Data that we disclosed for a business purpose, and the categories of recipients to which we disclosed that Personal Data.
 - The specific pieces of Personal Data we have collected about you.
- **Right to Access, Confirm and Data Portability.** You may have the right to confirm whether we are processing your Personal Data, to access your Personal Data, and to obtain a copy of Personal Data you provided to us in a portable format.
- **Right to Delete.** You may have the right to delete the Personal Data that we have collected from you, subject to certain exceptions.
- **Right to Correct.** You may have the right to request that we correct inaccuracies in your Personal Data, taking into account the nature of the Personal Data and our purposes for processing it.
- **Right to Opt Out of Sales and Sharing of Personal Data for Targeted Advertising.** You may have the right to opt out of the sale of your Personal Data, and to request that we do not share your Personal Data for targeted or cross-context behavioral advertising.
- **Right to Withdraw Consent or Limit Use and Disclosure of Sensitive Personal Data.** If we process Sensitive Personal Data from you, you may have the right to withdraw a previously provided consent for processing your Sensitive Personal Data for a specific purpose. For California residents, we do not use or disclose Sensitive Personal Data for purposes to which the right to limit use and disclosure applies.
- **Right to Know Third Party Disclosures.** You may have the right to request a list of third parties to which we have disclosed Personal Data.
- **Rights Related to Automated Decision-Making or Profiling.** We do not use your information for profiling in furtherance of decisions that produce legal or similarly significant effects or for the purposes of automated decision-making as defined under currently applicable law.
- **Right to Appeal.** Sometimes we are unable to process requests relating to your Personal Data, in which case, your request will be denied. If you have previously submitted a privacy rights request to us that has been denied and you believe that we denied it in error, you may have the right to appeal for reconsideration of your request by emailing us at privacy@outbrain.com or by calling us toll free on 1-866-I-OPT-OUT and entering service code 253# to leave us a message.
- **Non discrimination.** You are entitled to exercise the rights described above free from discrimination.

b) How to exercise your rights

You may exercise your privacy rights described above as follows:

- By calling us toll free on 1-866-I-OPT-OUT and entering service code 253# to leave us a message.
- By emailing privacy@outbrain.com

c) Right to opt-out of the “sale” or “sharing” for targeted advertising of your Personal Data.

We do not sell your Personal Data in the conventional sense (i.e., for money). However, like many companies, we use services that help deliver interest-based ads to you. To opt-out from this “sale” or “share” for targeted advertising, click on this [link](#) which will take you to our Interest Profile where you can opt out of personalized recommendations. If you choose to use the Global Privacy Control (GPC) browser signal, you will only be opted out of online sales or sharing of Personal Data, and will need to turn it on for each browser you use.

We will need to confirm your identity and state of residency to process your requests. We cannot



process your request if you do not provide us with sufficient detail to allow us to understand and respond to it. Depending on your state of residency, you may be able to designate an authorized agent to make a request on your behalf; however, you may still need to verify your identity with us before your request can be processed. An authorized agent may submit a request on your behalf using the methods listed above.

Please note that if you make a privacy rights request, we will retain the Personal Data submitted in connection with your request for recordkeeping purposes.

d) Personal Data that we collect, disclose, sell and share

The section below summarizes how we collect, disclose, sell and share Personal Data, and describes our practices during the 12 months preceding the effective date of this Privacy Policy as well as our current practices. These examples may vary depending on the nature of your interactions with us. Additional information may be found in this Outbrain Privacy Policy.

We collect the following categories of Personal Data about you, as described more fully in this User Privacy Policy above:

- Identifiers
- Internet or Network Information
- Geolocation Data
- Inferences

For information on the various sources from which we collect these categories of Personal Data, as well as the purposes of our collection and use, please refer to Section 3 of the Outbrain Privacy Policy above.

We may disclose the categories of Personal Data listed above to our affiliates, service providers and contractors for the following business purposes:

- Services performed on our behalf (including processing, maintaining, or collecting Personal Data) related to the operation of our business
- Auditing relating to ad impressions
- Ensuring security and integrity of Personal Data
- Debugging to identify and repair errors that impair existing intended functionality
- Short-term, transient use, including but not limited to, non-personalized advertising
- Advertising or marketing services performed on our behalf
- Undertaking internal research for technological development and demonstration
- Undertaking activities to verify or maintain the quality or safety of our services

e) Targeted Advertising, Sales, and Sharing of Personal Data

Although we do not sell Personal Data in exchange for money, some of the ways in which we share Personal Data for targeted or cross-context behavioral advertising or analytics may be considered “sales” or “sharing” under certain United States state privacy laws. Please see [here](#) for a list of our trusted partners. .

The purposes for which we sell/share this information include to deliver interest-based ads to you. We do not have actual knowledge that we sell or share the Personal Data of consumers under the age of 16.

10. “Do Not Track” disclosure

Some browsers transmit Do Not Track (DNT) signals to websites. Because there is no common understanding of how to interpret the DNT signal, Outbrain does not currently alter, change, or respond to DNT requests or signals from these browsers. We will continue to monitor industry activity in this area and reassess our DNT practices as necessary. In the meantime, you can use the range of other tools we provide to control data collection and use, including the ability to opt out of receiving personalized recommendations in the Users section. We also recognize the GPC browser signal, as described in Section 9 above.



11. **Contact us**

a) Data Protection Officer (DPO) - if you are based outside the US

To communicate with our Data Protection Officer, please email at dpo@outbrain.com or use the contact details below. You may also contact your local data protection authority. A list of local data protection authorities is available [here](#).

b) General questions

If you have any questions or concerns about your privacy you may contact us at:

Outbrain Inc.

111 West 19th Street

3rd Floor

New York, NY 10011, USA

Attn: Privacy questions

Email: privacy@outbrain.com or dpo@outbrain.com