PRIVACY POLICY

Last Updated 30 October 2023

Outbrain is committed to protecting your personal data. This privacy policy ("Privacy Policy") governs Outbrain's use of data collected by us, including any and all personal data. Personal data is information that relates to you and may identify you as an individual. 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.

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

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.

What we do:

Outbrain's mission is to serve interesting recommendations to you based on what we believe are your 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);
- advertisers who want readers to view their content (this is Outbrain Amplify); and
- third party partners who help us serve relevant recommendations.

For further information on our Amplify (advertiser) services see here and our Engage (publisher) services see here.

How to contact us:

We regularly review our compliance with this Privacy Policy. Questions, comments and requests regarding this Privacy Policy are welcomed and should be addressed in the first instance to privacy@outbrain.com or by mail to *Outbrain Inc., 111 West 19th Street, 3rd Floor, New York, NY 10011, USA, Attn: Privacy Questions*.

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 ; and/or
- the Information Commissioner's Office , which is Outbrain's supervisory authority in the UK.
- 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

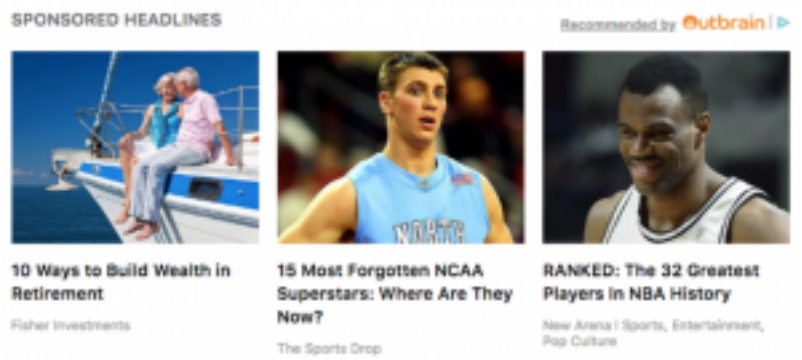
- We are also TAG Brand Safety Certified here.

3. Outbrain User Types (including Opt Out Options)

Much of this Privacy Policy is divided into sections based on the way you may interact with Outbrain. You are either a Site Visitor, a User and/or a Business Partner (as defined below). Please determine what user type you are. For each user type we've explained what information we collect and why, what cookies and other similar technologies we use, how we share such information and your rights.

Users: You are a User when you visit a page of a website or application of one of Outbrain's 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 text referencing Outbrain (e.g., "Recommended by Outbrain", "by Outbrain" near recommendations If you click on the hyperlinked reference to Outbrain you will see a detailed notice that enables you to navigate to Outbrain's Interest Portal and this Privacy Policy where you can opt out of personalized recommendations. In some instances, a partner may have white-label 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



See more here.

(a) What information we collect and why

We use UUIDs, IP Address and other Usage Information so that we can serve interesting recommendations. 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. Outbrain may use high-level health interest categories to serve recommendations, that you can find here.

- **UUID**

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.

- **IP Address**

In addition to your UUID, we recognise your IP address, which we translate into geolocation and delete the last octet in order to mask the identifying information. We then use this masked information, 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 recognise your IP address even if you opt out of personalised 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 (a) 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 (b) 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); (iii) operating system version; and (iv) device model (e.g. iPhone X).This information is considered personal data if Outbrain associates it with a UUID.

As Outbrain does not have a direct relationship with Users interacting with Partner Sites, Outbrain relies on its partners to determine the lawful basis upon which Outbrain can process personal data. Each partner site relies on either

(b) What cookies and other similar technologies we use

- **Outbrain cookies**

Please see the Cookie Table under “Users” for a detailed list of the First Party Cookies we use when you interact with Partner Sites where the Outbrain technology is implemented.

- **Outbrain pixels**

In addition to Outbrain’s visible widget on Partner Sites, certain Outbrain advertisers may implement the Outbrain pixel on their websites. The Outbrain pixel determines whether the User reaching the page where the pixel is installed has an Outbrain UUID in order to provide reporting to advertisers in respect of their particular campaign. 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 anonymised 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. Outbrain does not combine information received from the Outbrain pixel information with a UUID’s profile (for example, Outbrain only tracks that 1 conversion has taken place and not the UUID123 has converted when it reaches the advertiser’s chosen page). We require advertisers 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). Any such collection shall be governed by such third parties privacy policy.

- **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.

(c) How we may share information

- **Our Partners**

Outbrain does not share and/or sell a User’s entire profiles with any third parties. However, we may share certain elements of a user profile (for example, UUID) with the following partners, including:

1. Brand safety, analytics and fraud partners;
2. Demand Side Platforms (DSP) and Supply Side Platforms (SSP);
3. Ad Exchanges and/or Networks; and
4. Demand Management Platforms.

Please see here for a list of some of our trusted partners. 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.

(d) Your rights

- **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 provides a general visualization of the data Outbrain knows about you and may use to make its recommendations.

- **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 personalised tracking on your applications. This opt out must be done via your device settings.

- **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, http://www.aboutads.info/choices; DAAC, www.youradchoices.ca/choices , and/or EDAA www.youronlinechoices.eu). 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.

IMPORTANT INFORMATION

Even though you have opted out of Outbrain's personalised 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.
- **You must not opt in to Outbrain for at least 21 days as the deletion of your profile is tied to your UUID.** Your opt out from Outbrain's personalized recommendations is effective immediately. However, if your browser permits local storage and you opt into Outbrain's personalized recommendations (for example, by accepting a cookie banner) within 21 days of your opt out, it is possible your prior profile will be reconnected to your UUID. If you do not opt in within 21 days, your profile will be deleted and cannot be recovered.
- **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 personalised 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.

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

Security

Outbrain has a dedicated security team. We maintain tight controls over the personal data we collect, retaining it in firewalled and secured databases with strictly limited and controlled access rights, to ensure it is secure. Please see our security standards for more information.

Business Partners have access to certain password-protected features of the Amplify or Engage service. Business Partners are responsible for keeping this password confidential and for ensuring the same for their employees and/or their agents. 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.

Data Transfers Outside the EU/EEA

When we transfer personal data from the European Economic Area (EEA) we will ensure such transfers are in compliance with relevant data protection laws, including, if applicable, EU Standard Contractual Clauses, or a European Commission positive adequacy decision under Article 25(6) of Directive 95/46/EC or Article 45 of the GDPR. In other words, your rights and protections remain with your data and we used 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.

Sharing

In addition to the description of how we may disclose your personal data for each user type, 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); and/or
- To respond to a genuine emergency.

In addition, we combine your personal data with those of other users in order to share trend information and aggregate user statistics with third parties, always in aggregated and anonymized form.

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. Outbrain also maintains a Data Retention Policy that details the retention period for personal data based on our analysis of how long the specific data is reasonably required for legal or business purposes. When we no longer need personal data, we securely delete or destroy it. Aggregated data, which cannot identify a device/browser (or individual) and is used for purposes of reporting and analysis, is maintained for as long as commercially necessary.

5. Children and Sensitive Data

Children

None of our services are intentionally directed at children under 16. We do not knowingly collect personal data from anyone under 16 years of age. If we determine upon collection that a Site Visitor, a User or a Business Partner is under 16, we will not use or maintain his/her 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. If you're a kid, please go play in the yard, don't use or interact with Outbrain!

Sensitive data

We do not collect or receive any sensitive categories of personal data.

6. European Territory Visitors

In compliance with certain privacy laws, in particular the European General Data Protection Regulation (GDPR), Outbrain provides specific additional rights for individuals who interact with Outbrain such as the right to access, rectification, right to object, to complaint, erasure and blockage. 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 demand that personal data is rectified or amended.
- the right to request that personal data should be deleted.
- the right to demand that the processing of personal data should be restricted.
- 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.
- 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.
- the right to complain to the responsible supervisory authority if believed that the processing of your personal data is in violation of the legislation.

In addition to the above, we reference certain rights for European Territory citizens throughout this Privacy Policy. Pursuant to the GDPR, citizens from "European Territories" mean the European Economic Area (EEA), the European Free Trade Area (EFTA) and Switzerland. For the purpose of this Privacy Policy, the term "European Territories" shall continue to include the United Kingdom, even after the United Kingdom leaves the European Economic Area following Brexit. If you are in the UK, or the European Economic Areas, the controller of your data is Outbrain UK Limited.

Please email Privacy@outbrain.com with any questions about exercising any of the above rights.

7. California Privacy Rights

This section applies only to California residents. It describes how we collect, use and share Personal Information of California residents in operating our business, and their rights with respect to that Personal Information. For purposes of this section, " Personal Information" has the meaning given in

the California Consumer Privacy Act of 2018 (“ CCPA”) but does not include information exempted from the scope of the CCPA.

(a) Your California privacy rights.

As a California resident, you have the rights listed below. However, these rights are not absolute, and in certain cases we may decline your request as permitted by law.

- **Information.** You can request the following information about how we have collected and used your Personal Information during the past 12 months:
    - The categories of Personal Information that we have collected.
    - The categories of sources from which we collected Personal Information.
    - The business or commercial purpose for collecting and/or selling Personal Information.
    - The categories of third parties with whom we share Personal Information.
    - Whether we have disclosed your Personal Information for a business purpose, and if so, the categories of Personal Information received by each category of third party recipient.
    - Whether we’ve sold your Personal Information, and if so, the categories of Personal Information received by each category of third party recipient.
- **Access.** You can request a copy of the Personal Information that we have collected about you during the past 12 months.
- **Deletion.** You can ask us to delete the Personal Information that we have collected from you.
- **Opt-out of sales.** If we sell your Personal Information, you can opt-out. In addition, if you direct us not to sell your Personal Information, we will consider it a request pursuant to California’s “Shine the Light” law to stop sharing your personal information covered by that law with third parties for their direct marketing purposes.
- **Opt-in.** We contractually prohibit our publishing and advertising clients from placing our technology on pages that target individuals younger than 16 years old. If we learn that you are younger than 16 years old, we will asking for your permission (or if you are younger than 13 years old, your parent or guardian’s permission) to sell your Personal Information before we do so.
- **Non discrimination.** You are entitled to exercise the rights described above free from discrimination. This means that we will not penalize you for exercising your rights by taking actions such as denying you services; increasing the price/rate of services; decreasing service quality; or suggesting that we may penalize you as described above for exercising your rights.

(b) How to exercise your rights

You may exercise your California privacy rights described above as follows:

- **Right to information, access and deletion**. You can request to exercise your information, access and deletion rights by:
    - calling us toll free on 1-866-I-OPT-OUT and entering service code 253# to leave us a message.
    - emailing privacy@outbrain.com
    - using the web form to submit your request(s) to us
- **Right to opt-out of the “sale” of your Personal Information**. We do not sell your Personal Information in the conventional sense (i.e., for money). However, like many companies, we use services that help deliver interest-based ads to you. California law classifies our use of these services as a “sale” of your Personal Information to the companies that provide the services. This is because we allow them to collect information from our website users (e.g., online identifiers and browsing activity) so they can help serve ads more likely to interest you. To opt-out from this “sale”, click on this link which will take you to our Interest Profile where you can opt out of personalised recommendations.

We will need to confirm your identity and California residency to process your requests to exercise your information, access or deletion rights. We cannot process your request if you do not provide us with sufficient detail to allow us to understand and respond to it.

(c) Personal information that we collect, use and share

The chart below summarizes how we collect, use and share Personal Information by reference to the statutory categories specified in the CCPA, and describes our practices during the 12 months preceding the effective date of this Privacy Policy. Categories in the chart refer to the categories described above in the general section of this Privacy Policy.

Outbrain User Type	Statutory category of personal information (PI) (click for details)	Source of the PI	Purpose for collection	How we may share, disclose or "sell" information.
Site Visitors	Identifiers Online Identifiers Geolocation Data Inferences Internet or Network Information	Site Visitor	See Section 2(a) (Site Visitors).	See Section 2(c) (Site Visitors).
Users	Identifiers Online Identifiers Geolocation Data Inferences Internet or Network Information	Users	See Section 2(a) (Users).	See Section 2(c) (Users).
Business Partners	Identifiers Financial Information	Business Partners	See Section 2(a) (Business Partners).	See Section 2(c) (Business Partners).

8. "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.

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

Outbrain 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 Principles shall govern. To learn more about the Data Privacy Framework (DPF) program, and to view our certification, please visit https://www.dataprivacyframework.gov/

Please click here to view our certification.

9. **Complaint and Dispute Resolution Procedure under the DPF**
Outbrain's internal complaints mechanism
In compliance with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF, Outbrain commits to resolve DPF Principles-related complaints about our collection and use of your personal information. EU and UK individuals with inquiries or complaints regarding our handling of personal data received in reliance on the EU-U.S. DPF and the UK Extension to the EU-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 and the UK Extension to the EU-U.S. DPF, Outbrain commits to refer unresolved complaints concerning our handling of personal data received in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF to Judicial Arbitration and Mediation Services, Inc. (JAMS), an alternative dispute resolution provider based in the United States. If you do not receive timely acknowledgment of your DPF Principles-related complaint from us, or if we have not addressed your DPF Principles-related complaint to your satisfaction, please visit JAMS for more information or to file a complaint. The services of JAMS are provided at no cost to you. Please contact or visit the https://www.jamsadr.com/DPF-Dispute-Resolution for more information or to file a complaint.

The Federal Trade Commission has jurisdiction over Outbrain's compliance with the EU-U.S. Data Privacy Framework (EU-U.S. DPF) and the UK Extension to the EU-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

(1) has previously been subject to binding arbitration;
(2) was the subject of a final judgement entered in a court action to which the individual was a party; or
(3) was previously settled by the parties.

For more details, please click here.

European Individual Rights Under The DPF
Outbrain must provide you:

- Information on the types of personal data collected
- Information on the purposes of collection and use
- Information on the type or identity of third parties to which your personal data is disclosed
- Choices for limiting use and disclosure of your personal data
- Access to your personal data
- Notification of the organization's liability if it transfers your personal data
- Notification of the requirement to disclose your personal data in response to lawful requests by public authorities
- Reasonable and appropriate security for your personal data
- A response to your complaint within 45 days
- Cost-free independent dispute resolution to address your data protection concerns
- The ability to invoke binding arbitration to address any complaint that the organization has violated its obligations under the DPF Principles to you and that has not been resolved by other means

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 information 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 information 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. How This Privacy Policy May Change

We may change this Privacy Policy from time to time. We will place a prominent notice that will be visible to you as a Site Visitor or Business Partner, but we do not have a means of advising Users of an update by way of notice. You should check back here periodically to see if the Privacy Policy has been updated as we will always show the date of the latest modification of the Privacy Policy at the top of the page so you can tell when it was last revised.

Data Protection Officer (DPO)

To communicate with our Data Protection Officer, please email at dpo@outbrain.com or use the contact details below.

Contact us

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

You may also contact your local data protection authority. A list of local data protection authorities is available here.