**Taboola Workplace Data Use Policy**

Last Updated: 11 October 2024

Dear Taboolars,

At Taboola, our employees are our top priority. We are glad to have you as a member of our team! Every permanent and non-permanent employee, former employee, contractor, consultant, temporary worker, intern, and volunteer (“Taboolar”, “you”, or “your”) has an important role in our operations and we value the abilities, experience, and background that each brings.

This Workplace Data Use Policy describes how Taboola, its subsidiaries, affiliates, and related entities (collectively referred to herein as “Taboola”, the “Taboola Corporate Group”, “we”, “us” or “our”) collect and process your personal data about you during and after your employment with us. Specifically, it describes the categories of personal data that we collect, how we use your personal data, how we secure your personal data, when we may disclose your personal data to third parties, and when we may transfer your personal data outside of your home jurisdiction. We also describe your rights regarding the personal data that we hold about you and how you can access, correct, and request erasure of your personal data. Additionally, we include practices and procedures on how you should use and protect our customer and partner personal data.

For purposes of this Workplace Data Use Policy, “Personal Data” includes any information about an identifiable individual. Personal Data does not include anonymous, de-identified data not associated with a particular individual. We will refer to your Personal Data herein as “Taboolar Data.”

Quick References

[Global Workplace Privacy Notice 2](#_Toc175223653)

[Internal Data Handling Policy 19](#_Toc175223654)

[EEA Data Subject Rights Handling Policy 30](#_Toc175223655)

[PRC Data Subject Rights Handling Policy 40](#_Toc175223656)

# Global Workplace Privacy Notice

1. *Introduction*
	1. Taboola respects the privacy rights of our permanent and non-permanent employees, former employees, contractors, consultants, temporary workers, interns, and volunteers ("Taboolars", “you”, “your”), and we are dedicated to providing transparency around the ways that we interact with your data. Taboola collects, uses, and discloses Personal Data as specified by the laws of the countries in which our Taboolars reside. This Global Workplace Privacy Notice (the “Privacy Notice”) applies to everyone who performs work for Taboola, anywhere around the globe.
	2. This Privacy Notice outlines Taboola’s standards for processing Taboolar Data. This Privacy Notice sets forth Taboola’s obligations to protect Taboolar Data, but it does not replace any specific data requirements that may apply to Taboola’s corporate functions or business units, which are simultaneously in effect. If there is a discrepancy between these requirements, the most protective provision will apply.
	3. If you have any questions or would like to discuss anything in this Privacy Notice, please do not hesitate to reach out according to the contact details in [Section 9 below](#bookmark=id.1fob9te).
2. *Taboolar Data We Collect and Our Legal Basis*
	1. **Personal Data We Collect Directly From Taboolars**
	2. In connection with your employment with Taboola, we may collect the following types of Personal Data about you, your dependents, and other individuals that you inform us are connected to you:

(a) Identification data – such as your name, surname, gender, photograph, date of birth, Taboolar identification number, signature., and languages.

(b) Contact details – such as your home address, telephone number, email addresses, beneficiaries, and emergency contact details.

(c) Employment details – such as your job title, department, office location, hire date, work permit information, employment contracts, performance and disciplinary records, grievance procedures, training records, sickness and holiday records.

(d) Educational and professional background – such as your academic and professional qualifications, education, CV or résumé, reference letters and interview notes.

(e) National identifiers – such as your social security number, national ID or passport, immigration status and documentation, visas, and national insurance numbers.

(f) Spouse and dependent information – such as, children information, your marital status.

(g) Financial information – such as banking details, tax information, wage and payroll information, withholdings, salary, benefits, expenses, company allowances, direct deposit information, and stock and equity grants.

(h) IT information – information required to provide access to Taboola's IT systems and networks such as IP addresses, log files, login information, and software/hardware inventories. Security information -- such as access card usage (to enter Taboola’s offices) and closed-circuit televisions (“CCTV”) footage. For further information about how we process IT and security information, see [Section 7 below](#bookmark=id.30j0zll).

(i) Taboolar photographs and video footage (for example, in our human resources databases, from company events and security camera footage).

(j) Benefit information and any forms related to applications for, or changes to, Taboolar health and welfare benefits (including, short-term and long-term disability, medical and dental care).

(k) Other information you choose to share with us – such as your hobbies and social preferences etc.

We will normally collect above Taboolar Data from you only (i) where we need the Taboolar Data to carry out our employment contract with you, (ii) where we need the Taboolar Data to comply with our legal obligations or exercise rights in the field of employment, (iii) where we have obtained your consent, or (iv) where the processing of Taboolar Data is in our legitimate interests and does not override your data protection interests or your fundamental rights and freedoms. In some cases, we may need the Taboolar Data to protect your vital interests or those of another person (for example, we may need to share your Taboolar Data with third parties in the event of a work-related emergency).

**Sensitive Taboolar Data**: We may also collect certain demographic data that qualifies as sensitive Taboolar Data, such as race, ethnicity, sexual orientation, and disability to help us understand the diversity of our workforce, provide work-related accommodations, manage absences from work, or conduct background checks necessary for the Taboolar’s role in advance of employment. We may also collect dietary restriction information for work events and clothing size information for Taboola work-based initiatives and giveaways. This information, when collected, is generally done so on a voluntary, consensual basis, and Taboolars are not required to provide this information, unless it is necessary for us to collect such information to comply with our legal obligations. We also may need to process sickness absence information to manage absences from work and comply with our legal obligation to pay statutory sick pay. With respect to Taboolars in the European Union, United Kingdom and Turkey, race, ethnicity, and diversity data is not collected.

* 1. **Personal Data We Collect from Third Parties**

In some cases, we may collect Personal Data about Taboolars from trusted third parties. For example, when we perform background checks that are necessary for the Taboolar’s role, we collect criminal records data (only for vetting purposes, where we have your consent and in accordance with applicable law) from background check providers.

We may also collect your identification, contact, employment and educational, security details above from professional recruiting firms, prior employers, professional social media websites (LinkedIn), [building management companies], or Taboola employees who recommended your candidacy in connection with your job application and hiring process. We will normally collect Taboolar Data in this paragraph from third parties only (i) where we need the Taboolar Data to carry out our employment contract with you, (ii) where we need the Taboolar Data to comply with our legal obligations or exercise rights in the field of employment, (iii) where the processing of Taboolar Data is in our legitimate interests and does not override your data protection interests or your fundamental rights and freedoms.

If we ask you to provide any other Personal Data not described above, then we will make clear to you what specific Personal Data we need and the reasons why we ask you to provide it.

1. *How We Use Your Taboolar Data*
	1. Taboola uses and discloses the Taboolar Data that we collect primarily for the purposes of managing our employment relationship with you, along with other business purposes, which may include:
		* 1. Recruitment;
			2. To understand whether we are meeting our diversity goals and how we can improve our practices going forwards;
			3. To determine eligibility for hiring (including the verification of references and qualifications);

(b) To administer payroll and benefits;

(c) To administer background checks when necessary for the role, where permitted by law;

(d) To process Taboolars’ work-related claims (such as workers’ compensation and insurance claims);

(e) To establish training and development requirements;

(f) To determine performance requirements and review work performance;

(g) To manage, plan, and organize workflow;

(h) To ensure health and safety in the workplace;

(i) To assess qualifications for a particular job or task;

(j) For disciplinary actions or terminations;

(k) To establish emergency contacts;

(l) To comply with laws and regulations (such as employment laws, health and safety laws, tax laws, and anti-discrimination laws), under judicial authorization, or to exercise or defend Taboola’s legal rights;

(m) To compile internal directories (such as Taboolar directories);

(n) To detect fraud or other types of wrongdoing;

(o) To ensure and administer the security of company-held information and Taboolar Data;

(p) For accounting, financial reporting, and business planning;

 (q) To monitor Taboola’s premises and communication facilities, including closed-circuit televisions (“CCTV”) cameras,

(r) To organize team-building activities and other Taboola-hosted events.

1. *How We Share Your Taboolar Data*
	1. We take care to allow your Taboolar Data to be accessed only by those who truly must access it in order to perform a service for the Taboolar or for Taboola, and to third parties who have legitimate purpose for accessing it. Whenever we authorize third parties to access your Taboolar Data, we take steps to ensure they have appropriate security measures in place and that they only use the Taboolar Data in confidence and in a way that is consistent with this Privacy Notice. When we share with these third parties, we do so on a need-to-know basis, under clear contractual terms (except with judicial bodies), and instructions for the processing of Taboolar Data.
	2. We may share your Taboolar Data in the following ways:

(a) **With other companies in the Taboola Corporate Group:** We may need to share your Taboolar Data with other Taboola offices around the world in order to manage and administer our human resources services, to manage Taboolar transfers and travel, and for other business purposes like IT, taxes, accounting, and general business management. These international companies in the Taboola Corporate Group may be registered by a different legal name than the company with which you are employed — for example, you may be employed by Taboola Korea Ltd. and we may need to share your Taboolar Data with Taboola (Thailand) Limited — but these companies all operate together as one global Taboola entity.

(b) **With third party service providers and agents:** We may also make certain Taboolar Data available to third parties who provide services to us (such as our human resource management software, benefits administrators, or pension plan, insurance, Taboolar benefit plan providers, payroll support services, share incentive plan and Taboolar stock purchase plan coordinators, and Taboolar travel management services). To organize team-building activities and other Taboola-hosted events, we may also share your information with event planners.

(c) **With third party companies that provide software and tools to Taboola:** We may also make certain Taboolar Data available to third party companies that provide tools relevant for our business operations (such as to assist with internal ticketing, product engineering, and design services). Should these companies require user log in details, those details will typically be limited to the Taboolar’s name and professional email.

(d) **With other third parties:** We may also share your information with other types of third parties, such as our legal representatives, industry groups, self-regulatory bodies, or judicial bodies (i) to comply with our legal obligations (including to comply with laws, regulations, and contracts, to respond to court orders, administrative or judicial process, subpoenas and search warrants, or to meet national security and law enforcement requests), (ii) to protect Taboola’s rights or property and/or (iii) to establish, exercise, or defend against potential, threatened, or actual litigation. We may share your information with third parties in connection with the sale, assignment, merger, or other reorganisation or transfer of all or part of our business. We may also share your information with other types of third parties to respond to an emergency that we, in good faith, believe requires us to disclose data to prevent harm. We may time to time receive requests from other companies, such as mortgage companies or future employers, to verify that you work with us or the details that you provide in your application.

* 1. We may transfer Taboolar Data to the third parties above;
1. where processing is necessary for the performance of an employment contract with you;
2. where processing is necessary for compliance with our legal obligation (including to comply with laws, regulations, and contracts, to respond to court orders, administrative or judicial process, subpoenas and search warrants, or to meet national security and law enforcement requests)
3. To establish, exercise, or defend against potential, threatened, or actual litigation;
4. the vital interests of the data subject or of another natural person; and/or
5. where the processing of Taboolar Data is in our legitimate interests and does not override your data protection interests or your fundamental rights and freedoms
6. In connection with the sale, assignment, merger, or other reorganisation or transfer of all or part of our business.
7. *International Transfers of Your Taboolar Data*
	1. *International Transfers to Service Providers and Third Parties:* Taboola and our service providers may collect, use, process, store, or disclose your Taboolar Data outside your home country or jurisdiction.  These outside countries may have different data protection laws than the laws of your home country. But rest assured that Taboola only transfers Taboolar Data to another country in accordance with applicable privacy laws, and where there are adequate data protections in place. When international personal data transfer is made to countries where there is no adequacy decision, Taboola relies on the European Commission’s approved Standard Contractual Clauses, which are contractual privacy and security commitments between companies that transfer personal data. We will ensure that your Taboolar Data is treated in accordance with this Privacy Notice wherever we process it.
	2. *International Transfers to Taboola Affiliates:* If you are a Taboolar in the EEA, the PRC, or California, Taboola may transfer your Taboolar Data outside of the country in which you work. To ensure that your Taboolar Data is adequately protected in such transfers, applicable data protection laws mandate that such transfers must take place using certain legal mechanisms. When transferring your Taboolar Data from the EEA or from the United Kingdom to Israel, Taboola relies on the European Commission’s determination or adequacy regulations of the UK that Israel offers adequate data protection for transfers from the EEA or the UK.

When transferring Taboolar Data from the EEA or PRC to elsewhere, Taboola relies on the European Commission’s approved Standard Contractual Clauses, which are contractual privacy and security commitments between companies that transfer Personal Data (for example, from Taboola Europe Limited to Taboola, Inc.). Similarly, where the UK GDPR applies, Taboola relies on “International Data Transfer Addendum to the EU Commission Standard Contractual Clauses” issued by the Information Commissioner under s.199A of the DPA 2018. Taboola.com Ltd. and its Affiliates have accordingly adopted Standard Contractual Clauses to ensure the legality, privacy, and security of the data flows necessary to provide, maintain, and develop our services.

1. *How Long We Keep Your Taboolar Data*
	1. We will keep your Taboolar Data for as long as is needed to carry out the purposes described above (or as otherwise required by law). Generally, this means we keep your Taboolar Data until the end of your Taboola employment, plus a reasonable period of time after to respond to any employment inquiries or to comply with applicable law, deal with any legal or administrative matters, or to provide you with ongoing pensions and other benefits. For further information about how long we keep Taboolar Data, please reach the Privacy Team.
2. *Monitoring Notice*
	1. We periodically need to monitor our IT and communications systems for specific purposes. We may do this through automated tools like anti-malware software, website filtering, spam filtering, intrusion detection and prevention systems, security software and mobile device management solutions to maintain and protect our IT systems and network security, including investigating and responding to suspected security incidents.
	2. We also monitor Taboola’s office premises by security footage and badge scans. For more detailed information about Taboola’s CCTV monitoring please see [Taboola CCTV Policy](https://brain.taboola.com/display/IITP/TABOOLA%2BCCTV%2BPOLICY).
	3. Where permitted by law, we may also monitor for other purposes, such as:

(a) To document and archive proof of business transactions;

(b) To train and evaluate our Taboolars;

(c) To protect our confidential information, intellectual property, and other business interests;

(d) To investigate breaches of our company policies or other unlawful or improper acts;

(e) To comply with a legal obligation; and

(f) For other legitimate purposes, as permitted by applicable law.

* 1. Please note that any Taboolar telephone conversations or transmissions, message, files, data, document, electronic communications, social media posts, internet access or usage, or any other types of information transmitted to or from, received or printed from, or created, stored, or recorded on our IT and communications systems and assets are presumed to be Taboola business-related and we may monitor it at any and all times and by any lawful means in accordance with this Privacy Notice.
	2. We recognise that any monitoring that we perform may impact our Taboolars' privacy, so we will always seek to ensure that any monitoring we perform is proportionate for the limited and specific purposes needed and conducted as required or permitted by applicable law. Before undertaking any monitoring activities, we will always consider your privacy carefully and assess whether there are any less invasive options available.
1. *Your Rights to Your Taboolar Data*
	1. Several of our self-service HR Information Systems (“HRIS”) (for example, Bamboo, SuccessFactors, and ADP) allow you to view and update some of the Taboolar Data that Taboola holds about you. If we have Taboolar Data that you cannot access via these HRIS tools, or if we have Taboolar Data that you believe is inaccurate or no longer relevant, and you would like us to correct or delete such data, then you may make a request via email to the privacy team or your designated human resources representative.
	2. If you are located in certain regions (including the EEA, PRC, Brazil, Thailand, and Turkey), you may have certain additional rights in relation to your Personal Data, such as:

(a) You have the right to request information about the Personal Data that we hold about you and its purpose, including information about how we process your personal data.

(b) You have the right to update, correct, and access your Personal Data.

(c) If we have collected and processed your Personal Data with your consent, then you have the right to withdraw your consent at any time. (Please note that withdrawing your consent will not affect the lawfulness of any processing we carried out prior to your withdrawal, nor will it affect processing of your Personal Data carried out in reliance on other lawful grounds other than consent).

(d) The right to object to processing of your Personal Data, ask us to restrict processing of your Personal Data, or request portability of your Personal Data.

(e) To have your Personal Data erased in a number of other circumstances, such as where it has been unlawfully processed, or where there are no overriding legitimate grounds for the processing.

(f) The right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

(j) To request compensation for damages in the event of damages incurred due to unlawful processing of personal data if you are a resident in Turkey.

* 1. You can make any of these requests by using the contact details provided in [Section 9 below](#bookmark=id.1fob9te). We will respond to all requests in accordance with applicable data protection laws.
1. *Questions and Concerns*
	1. If you have any questions or concerns about this Privacy Notice please contact Taboola’s Privacy Team at privacy@taboola.com, or your designated human resources representative as listed below:

 (a) In Asia: Anjali Oldfield, anjali.o@taboola.com

 (b) In Israel: Efrat Israeli-Korn, efrat.i@taboola.com

(c) In Europe: Anjali Oldfield, anjali.o@taboola.com

 (d) In the United States: Lana Saad, lana.s@taboola.com

 (e) In Brazil and Latin America: Natalie Coggins, natalie.c@taboola.com

* 1. If you are a Taboolar in the EEA, California, or PRC, you may also request to access and review our records of your Taboolar Data by emailing privacy@taboola.com. This shall provide notice to Taboola’s Privacy Team, human resources department, and Taboola’s appointed data protection officer (our “DPO”). You also have the right to reach out directly to our DPO by emailing DPO@taboola.com. Taboolars in the EEA also have the right to lodge any complaints or concerns with your local data protection authority (a “DPA”). You can find a list of all the European DPAs at <https://www.edpb.europa.eu/about-edpb/about-edpb/members_en>. Taboolars in the PRC also have the right to complain to the Cyberspace Administration of China.
1. *Updates to this Privacy Notice*
	1. We may update this Privacy Notice from time to time to reflect any changes in our privacy practices. Where the changes are material, we will inform all Taboolars by email and we will also indicate at the top of this Privacy Notice the date that it was last updated. We encourage you to check back periodically to make sure you're aware of the most recent provisions.
2. *Notice of Collection and Use of Taboolar Data for California Residents*
	1. Taboola may collect (and may have collected during the 12-month period prior to the effective date of this policy the following categories of personal information about employees who are California residents (“California Taboolar”).
		* 1. Identifiers: identifiers, such as a real name, alias, postal address, unique personal identifier (e.g., a device identifier, employee number, unique pseudonym, or user alias/ID), telephone number, online identifier, Internet Protocol address, email address, account name, Social Security number, driver’s license number, passport number, and other similar identifiers.
			2. Additional Data Subject to Cal. Civ. Code § 1798.80: signature, physical characteristics or description, state identification card number, insurance policy number, education, bank account number, credit card number and debit card number, and other financial information, medical information, and health insurance information.
			3. Protected Classifications: characteristics of protected classifications under California or federal law, such as race, national origin, age, gender, sex, marital status, medical condition, disability, citizenship status, and military and veteran status.
			4. Online Activity: Internet and other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding your interaction with websites or applications.
			5. Sensory Information: audio, electronic, visual, and similar information.
			6. Employment Information: professional or employment-related information, such as compensation, benefits and payroll information (e.g., salary-related information, tax-related information, benefits elections and details regarding leaves of absence), information relating to your position (e.g., job title and job description), performance-related information (e.g., evaluations and training), talent management information (e.g., résumé information, occupation details, education details, certifications and professional associations, historical compensation details, previous employment details, and pre-employment screening and background check information, including criminal records information), emergency contact information, and dependent information.
			7. Education Information: education information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. Sec. 1232g; 34 C.F.R. Part 99).
			8. Inferences: inferences drawn from any of the information identified above to create a profile about you reflecting your preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.
	2. Taboola may use (and may have used during the 12-month period prior to the effective date of this notice) personal information for the purpose of carrying out and supporting HR functions and activities, including the uses described below. In addition to these HR purposes, we list below relevant “business purposes” as they are described in the CCPA.
		* 1. Managing work activities and personnel generally, including recruiting; performing background checks; determining suitability for employment or promotion; determining physical and/or mental fitness for work; managing Taboolar onboarding; reviewing and evaluating performance; determining eligibility for and processing salary increases, bonuses, equity, and other incentive-based compensation; providing references; managing attendance, absences, leaves of absences, and vacations; administering payroll services; reimbursing expenses; administering health, dental, and other benefits; accommodating disabilities or illnesses; supporting wellness; training and talent development; facilitating employee relocations and international assignments; making travel arrangements; securing immigration statuses; monitoring staff; creating staff directories; managing Taboolar headcount, work planning, and office allocation; investigating suspected misconduct or non-performance of duties; managing disciplinary matters, grievances, and terminations; reviewing staffing decisions; providing access to facilities; managing communications and relations with California residents; and carrying out obligations under employment contracts.
			2. Ensuring business continuity; protecting the health and safety of our staff and others; managing emergency response; safeguarding, monitoring, and maintaining our IT infrastructure, office equipment, facilities, and other property; providing technical support; detecting or preventing theft or fraud, or attempted theft or fraud; and facilitating communication with you and your designated contacts in an emergency.
			3. Operating and managing our IT, communications systems and facilities, and monitoring the use of these resources; performing data analytics; improving our services; allocating and managing company assets and human resources; strategic planning; project management; compiling audit trails and other reporting tools; maintaining records relating to business activities, budgeting, and financial management; managing mergers, acquisitions, sales, reorganizations or disposals and integration with business partners.
			4. Complying with legal requirements, such as tax, record-keeping and reporting obligations; conducting audits, management and resolution of health and safety matters; complying with requests from government or other public authorities; responding to legal process such as subpoenas and court orders; pursuing legal rights and remedies; defending litigation and managing complaints or claims; conducting investigations; and complying with internal policies and procedures.
			5. Performing services, including maintaining or servicing accounts, providing services to California Taboolars, processing transactions and payments, verifying California Taboolars’ information, providing analytics services, providing storage, or providing similar services.
			6. Auditing, including auditing compliance.
			7. Certain short-term, transient uses.
			8. Helping to ensure security and integrity of our business resources.
			9. Debugging to identify and repair errors that impair existing intended functionality.
			10. Undertaking internal research for technological development and demonstration.
			11. Undertaking activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by us, and to improve, upgrade, or enhance the service or device that is owned, manufactured, manufactured for, or controlled by us.

Taboola does not use or disclose sensitive personal information with the purpose of inferring characteristics about California Taboolars.

To the extent we process deidentified information, we will maintain and use the information in deidentified form and will not attempt to reidentify the information unless permitted by applicable law.

* 1. Retention of Personal Information

Taboola retains personal information of California Taboolars for the period reasonably necessary to achieve the purposes outlined in this notice, or any other notice provided at the time of collection, unless a longer retention period is required or permitted by applicable law, taking into account relevant statutes of limitations and Taboola’s records retention requirements and policies.

* 1. Sources of Personal Information

During the 12-month period prior to the Effective Date of this notice, Taboola may have obtained personal information about California Taboolars from the following categories of sources:

* + - 1. Directly from you;
			2. Devices you use in connection with your employment or online interactions with us;
			3. Family or friends who provide information about you, for example, in connection with our provision of benefits or services;
			4. Customers or business partners who provide information about you, such as when they provide feedback;
			5. Our affiliates and subsidiaries;
			6. Vendors who provide services on our behalf;
			7. Internet service providers;
			8. Operators systems and platforms;
			9. Government entities;
			10. Social networks; and
			11. Data brokers, such as credit bureaus, credit reporting service providers and background check services.
	1. Disclosure of Personal Information

During the 12-month period prior to the Effective Date of this notice, Taboola may have disclosed the following categories of personal information about you for a business purpose to the following categories of third parties:

|  |  |
| --- | --- |
| **Category of Personal Information** | **Categories of Third Parties** |
| Identifiers | * Our affiliates and subsidiaries
* Vendors who provide services on our behalf
* Professional services organizations, such as auditors and law firms
* Business partners
* Internet service providers
* Operating systems and platforms
* Government entities
* Social networks
 |
| Additional Data Subject to Cal. Civ. Code § 1798.80 | * Vendors who provide services on our behalf
* Professional services organizations, such as auditors and law firms
 |
| Protected Classifications | * Vendors who provide services on our behalf
* Government entities
 |
| Online Activity | * Social networks
 |
| Sensory Information | * Social networks
 |
| Employment Information | * Our affiliates and subsidiaries
* Vendors who provide services on our behalf
* Professional services organizations, such as auditors and law firms
* Business partners
* Operating systems and platforms
* Government entities
* Data brokers
 |
| Education Information | * Our affiliates and subsidiaries
* Vendors who provide services on our behalf
* Operating systems and platforms Data brokers
 |
| Inferences  | * Social networks
 |

In addition to the categories of third parties identified above, during the 12-month period prior to the Effective Date of this notice, we may have disclosed personal information about California Taboolars to government entities, or to third parties in connection with corporate transactions, such as mergers, acquisitions or divestitures.

Taboola does not sell or share (for cross-context behavioral advertising purposes) personal information about California Taboolars.

We do not have actual knowledge that we sell or share the personal information of minors under 16 years of age.

* 1. California Consumer Privacy Rights

If you are a California Taboolar, you have certain choices regarding your personal information. You have the right to request that Taboola:

* + - 1. provide you with what Taboolar Data Taboola has collected about you, including the categories of personal information, the categories of sources from which the personal information is collected, the business or commercial purpose for collecting, selling, or sharing personal information (if applicable), the categories of third parties to whom Taboola discloses personal information, and the specific pieces of personal information Taboola has collected about you,
			2. correct your personal information, if that information is inaccurate,
			3. delete your personal information, and
			4. opt you out of the sale or sharing of your personal information (if applicable).
	1. How to Submit a Request. To submit an access, correction or deletion request, please contact us at privacy@taboola.com. To submit a request as an authorized agent on behalf of an individual, please email privacy@taboola.com with the subject line “Authorized Agent Request.”
	2. Verifying Requests. To help protect your privacy and maintain security, we will take steps to verify your identity before granting you access to your personal information or complying with your request. We may verify your identity by requiring you to sign into your employee account. If you do not have an employee account and you request access to, or deletion or correction of, your personal information, to verify your identity, we will require additional information from you, such as your date of birth, last four digits of your employee identification number, and information about your employment dates with Taboola. In addition, if you ask us to provide you with specific pieces of personal information, we may require you to sign a declaration under penalty of perjury that you are the California Taboolar whose personal information is the subject of the request. If you designate an authorized agent to make a request on your behalf, (1) we may require you to provide the authorized agent written permission to do so, and (2) for access, correction and deletion requests, we may require you to verify your own identity directly with us (as described above).
	3. Additional Information. If you choose to exercise any of your rights under the CCPA, you have the right to not receive discriminatory treatment by us. To the extent permitted by applicable law, we may charge a reasonable fee to comply with your request.
	4. How To Contact Us

If you have any questions regarding this notice or our privacy practices, please email us at privacy@taboola.com.

* 1. California Resident Consumer Requests
	2. During the previous calendar year, we received and responded to these types of Taboolar requests as follows:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Number received | Number complied with in whole or in part | Number denied | Median number of days to respond |
| Requests to Know/Access | 0 |  0 | 0 | 0 |
| Request to Correct | 0 |  0 |  0 | 0 |
| Requests to Delete | 0 | 0 | 0 | 0 |
| Requests to Limit Use of Sensitive Personal Information | 0 |  0 | 0 | 0 |
| Requests to Opt-Out of The Sale/Share of Personal Information | 0 | 0 | 0 |  0 |

# Internal Data Handling Policy

1. *Introduction*
	1. Taboola has issued this Internal Data Handling Policy ("Data Handling Policy") for permanent and non-permanent employees, former employees, contractors, consultants, temporary workers, interns, and volunteers (each an “Taboolar”, "you", or "your").
	2. Taboola respects the Personal Data and data protection rights of all individuals (including our Taboolars, partners, clients, and potential clients), and we are fully committed and legally obligated to comply with applicable data protection laws. Because the Taboola Corporate Group is comprised of Taboola’s many global offices and registered entities, and because Taboola engages in business across all corners of the globe, Taboola has determined that EU data protection laws, and specifically the General Data Protection Regulation 2016 (the “GDPR”), offers individuals the greatest data protections as it relates to handling of Personal Data. Thus, we determined that our global operations shall comply with these standards.
	3. This Data Handling Policy explains what Taboolars must do when handling Personal Data found in Taboola’s contracts, Personal Data about **clients and professional contacts**, and Personal Data provided by **suppliers and colleagues.** Please address any questions or comments about this Data Handling Policy to Taboola’s Privacy Team, at privacy@taboola.com.
2. *Terminology Used in this Data Handling Policy*
	1. "Personal Data" means any information about an identified or identifiable natural person. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number, location data, online identifier, or to one or more factors specific to that person's physical, physiological, genetic, mental, economic, cultural or social identity.
		* 1. Examples of data that may permit this kind of identification in the employment context:
				1. Identification data (such as name, address, date and place of birth, photograph);
				2. Contact details (such as telephone number, email, address);
				3. National identifiers (such as ID numbers, tax IDs/social security numbers, driver's licence number, passport number);
				4. Information about education and training (educational history, professional qualification and experience, professional organisations, publications); and
				5. Information about professional status (such as title, position, location).
			2. Examples of data that may permit this kind of identification of a client or partner:
				1. Name and contact details on our Customer Relationship Management (“CRM”) databases (including Salesforce, Taboola Ads, and our emailing platforms);
				2. Email addresses;
				3. IP addresses;
				4. Newsletter subscriptions; and
				5. Marketing preferences.
	2. “Data Subject” means individuals within the European Economic Area (“EEA”) whose data is processed by Taboola. Data Subjects include: (i) individuals who interact with Taboola’s Content Distribution Platform (“Users”); (ii) publishers, advertisers, and other content providers with whom Taboola has a contractual relationship, ("Customers"); and (iii) Taboola’s permanent and non-permanent employees, former employees, contractors, consultants, temporary workers, interns, and volunteers ("Taboolars") and job applicants.
	3. "Processing", "Process" or "Processed" means any operation or set of operations performed upon Personal Data, whether or not by automatic means.
3. Examples of data processing include:
	1. Collecting data;
	2. Recording data;
	3. Organising data;
	4. Storing data,
	5. Altering data;
	6. Retrieving data;
	7. Consulting data,
	8. Use of data;
	9. Disclosure by transmission of data;
	10. Transfer of data;
	11. Remote access to data;
	12. Alignment or combination;
	13. Blocking data;
	14. Erasing data; and
	15. Deleting data.
	16. “Sensitive Data” is a subset of Personal Data that contains information relating to a person's race or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data (for identifying a person), health data, and data about sex life or sexual orientation.
	17. “Criminal Records Data” means information relating to criminal convictions and offenses or related security measures.
	18. **“Security Incident”** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored, or otherwise processed.
4. *Overarching Data Protection Principles*
	1. At Taboola, we must ensure that we:
		* 1. Are legally entitled to process the Personal Data under data protection law ("Lawful Grounds");
			2. Are transparent with individuals about what Personal Data we process and why ("Transparency");
			3. Do not use Personal Data for any purpose other than for which it is collected ("Purpose Limitation");
			4. Collect the minimum Personal Data needed for the purpose it is collected ("Minimisation");
			5. Keep Personal Data accurate and up to date ("Accuracy");
			6. Respect and honor the data subject rights of individuals based in specific regions (see the [EEA Data Subject Rights Handling Policy](#bookmark=id.1y810tw) and the [PRC Data Subject Rights Handling Policy](#_PRC_Data_Subject) for more information) ("Data Subject Rights");
			7. Keep Personal Data secure when used both internally and when shared with third parties ("Security");
			8. Transfer (or allow the transfer of) Data Subject’s Personal Data only if we have put in place appropriate data transfer arrangements ("Data Transfers"); and
			9. Build data protection compliance (for example, compliance with the above principles) into any new project that involves Personal Data processing or new use of Personal Data ("Data Protection by Design").
5. *How Should You as a Taboolar Comply with Data Protection Principles in Everyday Practice?*
* Use your Taboola email account for all business correspondence — do not use your personal email account.
* Scale down the Personal Data you access to only what is necessary to perform your required tasks.
* Just because *you* can access certain Personal Data does not mean *everyone* *else* should. Before you share Personal Data with another Taboolar, be sure they *need* it and have the *right* to access and use it.
* Change your passwords regularly and at least every 6 months. Do not write them down.
* Be respectful of our Customer’s contact choices -- if a contact is marked as “DO NOT CONTACT” in Salesforce, please do not contact them.
* Encrypt Sensitive Data when necessary — for example, when saving to a flash drive or emailing it.
* Use secure Internet connections when accessing our organisation’s network.
* Lock your computer when you step away from it.
* Report suspicious-looking emails. Do not reply to them or open any links or attachments.
* You should not collect or use any Sensitive Data or Criminal Records Data unless this has been reviewed and approved by Taboola’s Privacy Team, at privacy@taboola.com.
* Be aware of our policies and reach out to privacy@taboola.com with any questions.
* Understand the different measures we have in place to protect Personal Data and know when to use them.
* If you spot a privacy issue, report it to privacy@taboola.com or IT@taboola.com.
1. *How Does Taboola Comply with Data Protection Principles in Everyday Practice?*

We Ensure that We Have Lawful Grounds to Process Personal Data

* 1. We only process Personal Data for purposes permitted under applicable data protection law. Permissible purposes include:
		+ 1. To comply with a legal obligation (for example, as an employer, we may be required to process certain information about our Taboolars);
			2. To protect the Data Subject’s vital interests (for example, if there is a medical emergency);
			3. For performance of a contract with the Data Subject or to perform steps prior to entering into a contract at the request of the data subject;
			4. For the legitimate interests of Taboola or a third party but only if the Data Subject’s rights are not outweighed, for example, where the business benefit to Taboola is limited but there would be significant intrusion on the privacy of the Data Subject; and/or
			5. The Data Subject has given his or her consent (although this should only be sought if one or more of the other grounds above do not apply).
	2. There are additional special grounds for processing Sensitive Data and data regarding criminal records. As noted above, you should not collect or use any Sensitive Data or Criminal Records Data unless it has been reviewed and approved by Taboola’s Privacy Team, at privacy@taboola.com.

Relying on Consent

Whenever relying on consent to process Personal Data, Taboola ensures that consent is:

* + - 1. Documented – so we can demonstrate that we have obtained consent lawfully;
			2. Given affirmatively (such as ticking a box or signing a document) – we cannot rely on 'inaction' as a way of obtaining consent (e.g., no pre-ticked boxes);
			3. Freely given and retractable at any time – it must be as easy for Data Subjects to withdraw their consent as it is to give their consent; and
			4. Not conditioned – for example, not given on the condition that other actions are taken, accepted, or exchanged.

Transparency, Purpose Limitation and Minimisation

* 1. You, as a Taboolar, should decide what Personal Data is necessary for the intended purpose (i.e. to provide the required business services) and collect only the minimal Personal Data necessary for that purpose.
	2. Because Personal Data may only be collected for a specific purpose, the Personal Data should only be retained for the time necessary to complete the purpose. Our Privacy Notices (internal and external) set forth the time period for which we generally retain Personal Data. Our computer and IT systems are already structured to comply with these timeframes for User personal data, so you should not tamper with these settings to keep the Personal Data for any longer. For the retention period of personal data of other data subject categories, please contact Taboola’s Privacy Team, at privacy@taboola.com.
	3. If you need to use Personal Data that Taboola has provided you with access to for any purpose other than approved legitimate business purposes, this must be reviewed and approved by Taboola’s Privacy Team, at privacy@taboola.com.

Accuracy

* 1. We must keep Personal Data accurate. This will mean, in each relevant context, that we must consider how we will regularly update information. If you get any such request from a client or partner, please direct this request to Taboola’s Privacy Team, at privacy@taboola.com.

Data Subject Rights

* 1. Taboola is required to immediately respond to any “Data Subject Access Requests” that we receive. So if you receive an inquiry from former employee, employee, customer, partner, or third party (i) asking what information or Personal Data Taboola holds about that individual, (ii) requesting that we update, restrict, delete, or correct that individual’s contact information or Personal Data, or (iii) if you receive complaints from individuals about Taboola’s processing of their Personal Data, please acknowledge receipt letting the individual know that you are passing their request to our privacy team and direct this **immediately** to Taboola’s Privacy Team, at privacy@taboola.com. Please remember that a data access request does not have to be official or mention data protection law to qualify as a valid request. If you are ever unsure, it is best to check with our Privacy Team.
	2. Data Subjects in the EEA and PRC are entitled to exercise certain rights with respect to their own Personal Data. These rights are explained in [Taboola’s EEA Data Subject Rights Handling Policy](#bookmark=id.1y810tw) and [Taboola’s PRC Data Subject Rights Handling Policy](#_PRC_Data_Subject).

Security

* 1. Taboola must keep Personal Data secure and protect it from any unauthorised access, accidental loss, damage, or destruction. You should ensure that you are familiar with, and that you follow, our security policies and procedures that are designed to protect our IT systems, our premises, and the data stored within them (including both confidential information and Personal Data). You must also follow the practical steps set forth [above in Section 4](#bookmark=id.tyjcwt).
	2. When Taboola collects Personal Data for a particular purpose, we must always consider whether we could achieve the same purpose with anonymised data. If that is not possible, we should strive to encrypt or pseudonymize the Personal Data (for example, by masking, hashing, or otherwise concealing the data). The more confidential the information, the higher our security standards will need to be to protect it. Please consult with Taboola’s Privacy Team, at privacy@taboola.com, if you have questions about whether certain Personal Data needs to be encrypted or pseudonymised.
	3. If you suspect any Security Incident, please contact the Privacy Team at privacy@taboola.com and the Security Team at security@taboola.com.

Data Sharing

* 1. Personal Data should not be shared with anyone or any organisation outside of the Taboola Corporate Group (including to our service providers) unless (i) appropriate contractual arrangements have been signed (including our standard non-disclosure and data processing agreement), or (ii) the disclosure is otherwise permitted under data protection law. Please consult with Taboola’s Legal team (legal@taboola.com) prior to sharing any Personal Data with any third party.
	2. Before authorizing any third party providers to hold or have access to Personal Data on our behalf, Taboola must first carry out due diligence to verify that the third party meets our data protection standards for Personal Data and is compliant with the GDPR’s requirements. Please refer requests for due diligence assistance to Taboola’s IT Team, at IT@taboola.com.

Data Transfers

* 1. Personal Data cannot be transferred outside of the EEA, unless the transfer is:
		+ 1. To a country approved by the European Commission as having adequate data protection laws to protect the Personal Data (there are only a handful of these); or
			2. To an organisation that has entered into a data transfer agreement with us (based on European Commission approved standard contracts).
	2. Personal Data cannot be transferred outside of the PRC, unless the transfer:
		+ 1. Is with the Taboolar’s consent to do so;
			2. Passed the security assessment organized by the PRC cyberspace administration;
			3. Has been certified in accordance with the provisions of the PRC cyberspace administration;
			4. Is to an oversees recipient that has entered into a data transfer agreement (based on a standard contract formulated by the PRC cyberspace administration, or until available, is in good faith based on best industry practices);
			5. Satisfied other conditions prescribed by laws, administrative regulations, or the PRC cyberspace administration.

If you are aware of any (planned) Personal Data transfers without at least one of the above mechanisms in place or to confirm that one of the above mechanisms is in place, please contact Taboola’s Legal Team, at legal@taboola.com.

Data Protection by Design and Data Protection Impact Assessments

* 1. Taboola must build data protection compliance into our processes and systems from the ground up. To do this, it is important that all Taboolars have a good understanding of our data protection obligations (as set out in this Data Handling Policy). It is also necessary to ensure that the concept of “Data Protection by Design” — or ensuring that new systems that that Taboola introduces are designed to minimize the Personal Data that they collect — is embedded into our product development processes and considered from the outset and throughout the life cycle of the product. This is especially important for our R&D, Product, and IT Taboolars to keep in mind as they perform their business tasks.
	2. We also have standard procedures and templates for carrying out a “Data Protection Impact Assessment” or “DPIA” — which is the process of evaluating and documenting the potential individual privacy risks that could result from Taboola’s new projects, processes, or product developments that involve the collection of Personal Data. For higher risk (more intrusive) uses of Personal Data, completing a DPIA may be required by data protection law. Please consult with Taboola’s Privacy Team, at privacy@taboola.com to determine whether your new project or product development task requires a DPIA.
1. *Data protection complaints*
	1. For instructions on how EEA Data Subjects may exercise their data subject rights, please see the [EEA Data Subject Rights Handling Policy](#bookmark=id.1y810tw). For instructions on how PRC Data Subjects may exercise their data subject rights, please see the [PRC Data Subject Rights Handling Policy](#_PRC_Data_Subject).
	2. For complaints from individuals about Taboola’s processing of their Personal Data, please immediately direct the complaint to Taboola’s Privacy Team, at privacy@taboola.com.
2. *Data Breach Management Policy*
	1. Companies that suffer from a Security Incident, including a data protection breach, can face (i) significant reputational harm; (ii) enormous fines; and (iii) claims from individuals for the breach of their data protection.
	2. Taboola needs to have in place a robust and systematic process for responding to any reported data security breach to ensure it can act responsibly and protect information assets as far as possible.
	3. Data security breaches include both confirmed and suspected incidents. The aim of this policy is to standardise Taboola’s response to any reported Security Incident and/or data breach, ensure they are appropriately logged and managed in accordance with best practice guidelines, ensure any breaches are contained, risks associated with the breach minimised and actions considered to secure personal data and prevent further breaches.
	4. Types of incident include, but are not restricted to: • Loss of confidential or sensitive data or equipment on which such data is stored (e.g. loss of laptop, USB stick, iPad, tablet device or paper record) • Careless document storage, display or retention leading to confidential personal data being visible to others on screen or on paper • Equipment theft or failure • System failure • Unauthorised use of, access to or modification of data on information systems • Attempts (failed or successful) to gain unauthorised access to information on IT system(s) • Unauthorised disclosure of sensitive / confidential data • Website defacement • Hacking attack • Unforeseen circumstances such as fire or flood • Human error • ‘Blagging’ offences where information is obtained by deceiving the organisation who holds it
	5. Responsibilities
* Under the GDPR, any confirmed or suspected data security breaches must be reported to the relevant supervisory authority within 72 hours (nonworking hours) of Taboola becoming aware of the incident. Therefore, all Taboolars are required to follow this procedure for reporting a Security Incident as soon as possible. Security Incidents are reported to the Security team in line with this procedure. The Security team is responsible for managing information security responses and notifying management and Legal.
* Sales and IT team undergo their information security and privacy trainings on the Bridge platform.
	1. Data Classification
	+ Data security breaches will vary in impact and risk depending on the content and the quantity of the data involved, therefore, it is important that Taboola is able to quickly identify the classification of the data and respond to all reported incidents in a timely and appropriate manner.
	+ All reported incidents will need to include the appropriate data classification in order for assessment of risk to be conducted. Data classification referred to in this policy means the following categories:
	+ Public – any information published or available publicly (in the public domain)
	+ Internal – any information circulated within Taboola only, including information which is only accessible to certain employees/groups/committee members/contracted parties
	+ Confidential – any personal or confidential information
	+ Protected – highly sensitive information.
	1. Procedure
* Security Incident is reported, immediately after they are seen or experienced, by sending an email to security@taboola.com, opening a JIRA ticket for “Security,” or reporting via phone to the local information security manager/trustee.
* The security team will investigate the Security Incident. The Security Incident will be investigated to determine whether a breach has occurred, by establishing whether personal data has been accidentally or unlawfully:
* Lost
* Stolen
* Destroyed
* Altered
* Disclosed or made available where it should not have been
* Made available to unauthorised people
* The security team will take the appropriate controls/mitigations needed to resolve it.
* If a data breach has been identified (unauthorized PII access, malicious intent, data destruction), the Information Security Manager will notify VP IT, Legal, CTO.
* The security team will work with the Legal team to consider the likelihood and severity of the resulting risk. If there is a likely risk, then the Legal team may notify the Data Protection Officer (DPO) for further assessment. If the risk is unlikely then the incident will be documented but not reported. This will be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people’s rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress) through: • Loss of control over their data • Discrimination • Identity fraud or theft • Financial loss • Unauthorised reversal of Pseudonymisation (for example key coding) • Damage to reputation • Loss of confidentiality • Any other significant economic or social disadvantage to the individual(s) concerned.
* If a breach is likely to result in a high risk to the rights and freedoms of individuals, the DPO will notify those affected without undue delay. This will help them to take any necessary steps to protect themselves from the effects of a breach. The notification will include:
* The name and contact details of the DPO
* A description of the likely consequences of the personal data breach
* A description of measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
* The breach will be documented, irrespective of whether the breach is reported to the relevant supervisory authority. For each breach this will include the: • The facts and cause of the breach • Any effects thereof • Action taken to minimise the breach and ensure as practicably as possible that it does not happen again (such as establishing more robust processes or providing further training for individuals)
* The Breach and Near Miss Log will be stored on Taboola’s network, with restricted access.
	1. All Taboolars shall comply with this Policy. Taboolar breaches of this Internal Data Handling Policy will be taken seriously and may result in disciplinary action.
	2. Review of Policy
* The policy and procedure will be reviewed in line with future legislative changes, case law or annually.

# EEA Data Subject Rights Handling Policy

1. *Introduction*

Taboola has issued this EEA Data Subject Rights Handling Policy to describe the practices and procedures that Taboola follows when it receives requests about our use of Personal Data from: (i) individuals who interact with Taboola’s Content Distribution Platform (“Users”); (ii) publishers, advertisers, and other content providers with whom Taboola has a contractual relationship, ("Customers"); and (iii) Taboola’s permanent and non-permanent employees, former employees, contractors, consultants, temporary workers, interns, and volunteers ("Taboolars"). Any individual User, Customer, or Taboolar in the European Economic Area, (“EEA”) whose data is processed by Taboola shall each be referred to hereinafter as a “Data Subject”.

1. *Rights That All Data Subjects Have Regarding Their Personal Data*

Data Subjects have data protection rights that they may exercise by making a request to Taboola (a “Data Subject Rights Request”). These data subject rights include the right to request:

* + - Access to their Personal Data;
		- Rectification or Correction of their Personal Data;
		- Erasure of their Personal Data (also referred to as the '*Right to be Forgotten*');
		- Restriction on Taboola’s processing of their Personal Data;
		- Portability of their Personal Data;
		- Termination of any further processing of their Personal Data (also referred to as the ‘*Right to Object*’);
		- Not to be subject to automated decision making; and
		- Not to be sent direct marketing.
	1. Each of these rights is described in more detail in [below](#bookmark=id.lnxbz9).
	2. The procedures described in this EEA Data Subject Rights Handling Policy outline how Taboola, as a data controller (the entity determining the purpose for which, and manner in which, the Personal Data is processed), will respond to any Data Subject Rights Requests.
1. *Responsibility to Respond to a Data Subject Rights Request*
	1. The controller of a Data Subject’s Personal Data is primarily responsible for responding to a Data Subject Rights Request and for facilitating the Data Subject’s exercise of his or her rights under applicable data protection laws. For example, because Taboola determines what data it will collect from its Taboolars, and how it will process this Taboolar data, Taboola is the controller of the Taboolar’s Personal Data that it holds and processes. As the controller of the Taboolar’s Data, Taboola must respond to any Data Subject Rights Request we receive from a Taboolar. As a second example, Taboola is a controller of the data that we collect from individuals (“Users”) who interact with the Taboola Content Discovery Platform because we determine the purposes for which the data is collected and the means by which it is processed. Therefore, Taboola must respond to any Data Subject Rights Request we receive from a User about the Personal Data that we collect through our Content Discovery Platform.
	2. In certain circumstances, Taboola may process a Data Subject’s Personal Data as a processor on behalf of a third party who is the controller (rather than for its own purposes). In such instances, Taboola must inform the relevant third party promptly and provide it with reasonable assistance to help the third party honor the Data Subject’s rights in accordance with applicable data protection laws.
2. *Personal Data That Taboola Has Made Available to Third Parties*
	1. If Taboola shares Personal Data with third parties, it is our responsibility to inform those third parties of any request we receive from Data Subjects to rectify, erase, or restrict their Personal Data, unless doing so would involve disproportionate effort or is impossible. For example, when Taboola receives a Data Subject Rights Request, we must notify any relevant Taboola entity, processors, or other third parties (such as occupational health providers) that we have disclosed the Personal Data to, so that they may also update their records accordingly. As a general rule, in order to comply with this requirement, Taboola requires that all of its processors erase any Personal Data they receive from T-aboola within thirty (30) days of their receipt of such Personal Data. If you have concerns about any service providers that you are engaged with, please consult with Taboola’s Legal Team, at legal@taboola.com. All Data Subject Rights Requests and questions that you receive from non-Taboolars should be sent to Taboola’s Privacy Team at privacy@taboola.com.
	2. If requested, Taboola must also provide the Data Subject with details about third parties to whom we have disclosed the Data Subject's Personal Data.
3. *Where Can You Send Your Own Data Subject Rights Requests and Questions?*
	1. If you are a Taboolar in the EEA, and you wish to make a Data Subject Rights Request regarding the Personal Data that Taboola holds about you, please send your request to privacy@taboola.com.
	2. Any questions regarding Taboolar Data Subject Rights Requests should also be sent to privacy@taboola.com.
	3. Users who engage with the Taboola Content Discovery Platform can make a Data Subject Rights Request [here](https://accessrequest.taboola.com/access/). All Data Subject Rights Requests and questions that you receive from non-Taboolars should be sent to Taboola’s Privacy Team at privacy@taboola.com.
4. *What to Do if You Receive a Data Subject Rights Request from a Taboolar or a Non-Taboolar Data Subject*
	1. If you receive a Data Subject Rights Request from another Taboolar, you should immediately direct the request to privacy@taboola.com. Please also include the date on which you received it, along with any other information that may help us efficiently respond to the request.
	2. If you receive a Data Subject Rights Request from a User who interacts with the Taboola Content Discovery Platform or from a Customer about a User request, you should (1) immediately refer the Data Subject to Taboola’s Data Subject Access Request Portal, available [here](https://accessrequest.taboola.com/access) and (2) immediately forward the request to Taboola’s Privacy Team, at privacy@taboola.com, and please also include the date on which you received it, along with any other information that may help us efficiently respond to the request.
	3. If you receive a Data Subject Rights Request about a Customer account, you should immediately direct the request to Taboola’s Privacy Team, at privacy@taboola.com. Please also include the date on which you received it, along with any other information that may help us efficiently respond to the request.
	4. European data protection legislation demands that Taboola respond to requests within a very short time frame, so it is crucial that you immediately direct any Data Rights Requests you receive to the appropriate person indicated above without delay.
5. *Verification Process*
	1. Taboola’s Privacy Team will assess every Data Rights Request that we receive to determine whether Taboola is the controller or a processor of the data requested. We may also need to verify that the request has been made by a genuine Data Subject (which may require that we request further identification of the requestor).
	2. If we determine that Taboola is a processor of the Data Subject’s requested data, and that one of Taboola’s Customers or another third party is the controller of this data, then Taboola shall notify the Customer or third party as soon as possible, per data protection regulations. Taboola shall also help the controller comply with the Data Subject Rights Request (in accordance with any contract terms which may be in place with the controller).
	3. If we determine that Taboola is the controller of the Data Subject’s requested data, Taboola shall contact the individual in writing to confirm receipt of the Data Subject Rights Request and seek confirmation of identity (if not already validated).
	4. If Taboola is not exempt under applicable data protection laws from fulfilling the Data Subject Rights Request, then Taboola, to the extent it deems necessary, will request any further information needed to action the individual's request. Once Taboola has all the information it needs to honor the Data Subject Rights Request, Taboola will respond to the request in accordance with Section 9, below.
6. *Exemptions from Requirement to Respond to a Data Subject Rights Request*
	1. Taboola is permitted to decline to honor a Data Subject Rights Request that is excessive or manifestly unfounded (for example, because repetitive requests have been made). In this case, Taboola must be able to demonstrate that the request is in fact, excessive or manifestly unfounded.
	2. In some cases, specific additional exemptions may apply. Where specific exemptions relating to particular Data Subject Rights Request exist, these are explained below.
	3. If Taboola is exempt from the requirement to fulfill a received Data Subject Rights Request, then Taboola will notify the individual that we intend to decline the Data Subject Rights Request and explain why an exemption applies. Taboolars should always forward inquiries to Taboola’s Privacy Team, at privacy@taboola.com, who can make an assessment about whether such an exemption applies. Please never make this determination yourself.
7. *Timeframe for Responding to a Data Subject Rights Request*
	1. Data Subject Rights Requests must be responded to without undue delay and in no case later than one month from the receipt of the request, unless this is not possible because the request is particularly complex. In such complex cases, Taboola will be entitled to extend its response period by up to two additional months. Within the initial month following receipt of the Data Subject Rights Request, Taboola must provide the Data Subject with notice of its intention to respond within this extended time period. The notice provided must explain the reasons for the delay. Given this short time frame for responding to Data Subject Rights Requests, it is imperative that you direct any requests that you receive immediately to Taboola Privacy Team, at privacy@taboola.com.
8. *Charging for Data Subject Rights Requests*
	1. Taboola is not legally permitted to charge for acting on a Data Subject Rights Request unless Taboola is exempt from the obligation to act on the request (see [Section 8, above](#bookmark=id.17dp8vu)) but is nonetheless prepared to act on the request anyway. In such a case, Taboola may charge the Data Subject a reasonable fee that accounts for the administrative costs of providing the information or communication or taking the action requested. Please consult with Taboola’s Privacy Team before seeking to impose any fees for responding to a Data Subject Rights Request.
9. *Requests for Access to Personal Data*

The Right of Access: This is a Data Subject’s right to obtain confirmation about whether his or her data is processed by a controller, and, if so, to be provided with details about and access to that Personal Data.

Information to be Provided in Response to a Right of Access Request

* 1. A Data Subject is entitled to request a copy of his or her Personal Data from Taboola. Where a Data Subject makes such a request, Taboola must confirm whether it holds and is processing Personal Data about that Data Subject and, if so, Taboola must provide that Personal Data to the Data Subject in an intelligible form.
	2. The Data Subject making the request should also be provided with the following information:
		1. A description of the Personal Data and categories of Personal Data concerned;
		2. The expected period for which the Personal Data will be stored;
		3. The purposes for which the Personal Data is being held and processed;
		4. The recipients or classes of recipients to whom the Personal Data is, or may be, disclosed by Taboola;
		5. Confirmation of the Data Subject’s right to request rectification or erasure of his or her Personal Data or to restrict or object to its processing;
		6. Confirmation of the Data Subject’s right to lodge a complaint with a competent data protection authority;
		7. Details about the source of the Personal Data, if it was not collected from the Data Subject;
		8. Details about whether the Data Subject’s Personal Data is subject to automated decision-making (including profiling); and
		9. Where Personal Data is transferred from the European Economic Area to a country outside of the European Economic Area, the appropriate safeguards that Taboola has put in place relating to transfers in accordance with European data protection laws.

Format of Requests

* 1. An access request does not have to be official or mention data protection law to qualify as a valid request. Please keep this in mind to the extent you receive any type of request from a User or Client — if you are not sure, it is best to check with Taboola’s Privacy Team, at privacy@taboola.com.
	2. An access request does not need to be made in writing and can be made orally but it is helpful if it is made in writing (for record keeping purposes). If made in writing it is also helpful if the Data Subject provides their email address and confirms whether the information can be sent to them by email (or other means by which they prefer to receive the information). Requests made electronically (e.g., by email) must be responded to electronically (in a commonly used format) unless the Data Subject stipulates otherwise. Data Subjects may ask for information to be provided orally instead. This is especially important for our human resources Taboolars to keep in mind, since they are most likely to receive oral requests from other Taboolars.

Exemptions

* 1. Taboola is not permitted to refuse to comply with an access request unless it can demonstrate that it is not in the position where we can identify the Data Subject who is making the request or Taboola is exempt from its obligations to comply (see [Section 8, above](#bookmark=id.17dp8vu), regarding exemptions).
1. *Requests to Rectify Personal Data*

The Right to Rectification: This is a Data Subject’s right to obtain rectification of inaccurate Personal Data that a controller may process about him or her.

Rectification by Taboola

* 1. If Taboola holds inaccurate or incomplete records of Personal Data about a Data Subject, the Data Subject is entitled to request that the Personal Data is rectified.

Rectification by Third Parties

* 1. If Taboola rectifies a Data Subject’s Personal Data, Taboola must also convey this rectification to any third parties that also use this Personal Data for processing purposes. See [Section 4, above](#bookmark=id.4d34og8).

Supplementary Statements to Complete Personal Data

* 1. Because a request to rectify Personal Data involves ensuring that the records are complete, the Data Subject may elect to provide a supplementary statement so that Taboola may complete the records of Personal Data held about them. This process is unlikely to happen in connection with Taboola’s Users, because we only hold their pseudonymized data. However, this may occur in connection with the Personal Data that we hold about our Customers or Taboolars.
1. *Requests to Erase Personal Data ("Right to be Forgotten")*

The Right to Erasure: This is a Data Subject’s right to require a controller to erase his or her Personal Data on certain grounds – for example, where the Personal Data is no longer necessary to fulfil the purposes for which it was collected.

Circumstances in Which Right to Erasure Applies

* 1. A Data Subject may request that Taboola erases his or her Personal Data in the following circumstances:
		1. The Personal Data is no longer necessary for the purpose for which it was collected or otherwise processed;
		2. The Personal Data was unlawfully processed by Taboola;
		3. If the processing was on the basis of the Data Subject’s given consent, and the Data Subject elects to withdraw his or her consent (and Taboola does not rely on any other legitimate interest grounds for our processing);
		4. The Data Subject objects to Taboola’s processing of his or her Personal Data (see [Section 14, below](#bookmark=id.44sinio)) and Taboola does not have any overriding legitimate interest grounds for continuing to process the information; and
		5. The Personal Data needs to be erased to comply with Taboola's legal obligations.
		6. Taboola’s Users may access and delete their Personal Data though Taboola’s Data Subject Access Request Portal, available [here](https://accessrequest.taboola.com/access).
		7. Taboola’s Customers may send an access or deletion request directly to our Taboolars. If you receive such a request from a Customer, please immediately direct it to Taboola’s Privacy Team, at privacy@taboola.com.
		8. Taboola’s EEA Taboolars should reach out to privacy@taboola.com to make any such requests.

Erasure of Personal Data by Processors

* 1. If Taboola erases a Data Subject’s information further to such a request, Taboola must also notify its processors. See [Section 4, above](#bookmark=id.4d34og8).
	2. If Taboola has made the Data Subject’s Personal Data public (for example, by publicly posting a photograph of a Taboolar or Customer from an event), and if Taboola is obliged to erase the Personal Data pursuant to a Data Subject Rights Request, Taboola must take reasonable steps, including technical measures (balancing its available technology and the cost of implementation), to inform processors that are processing the Personal Data that the Data Subject has requested that this Personal Data, and any links to, copies, or replicas, of the Personal Data be erased. This is most relevant for Taboolars in our Marketing Departments, so please consult with Taboola’s Privacy Team, at privacy@taboola.com, if you receive any erasure requests from Customers or potential customers following any marketing events.

Exemptions

* 1. In addition to the exemptions referred to above, Taboola is exempt from the obligation to erase Personal Data where its processing is necessary for:
		1. Compliance with Taboola's legal obligations;
		2. Establishing, exercising, or defending legal claims;
		3. Scientific, historical, or statistical purposes where erasure of the Personal Data would make this processing impossible or seriously impair it (please note that this exemption is unlikely to apply to Taboola).
1. *Right to Object to Processing*

The Right to Object: This is a Data Subject’s right to object to a controller’s processing of his or her Personal Data, if the controller is processing based on legitimate interest grounds.

Circumstances in Which Data Subjects May Object to Processing

* 1. A Data Subject may object to Taboola’s processing of his or her Personal Data, where Taboola relies on its legitimate business interests as the grounds for processing the Personal Data.

Exemptions

* 1. In addition to the exemption referred to above, Taboola is exempt from the obligation to cease further processing of a Data Subject’s Personal Data if:
		1. Taboola can demonstrate that we have compelling legitimate interest grounds for processing the Personal Data that override the interests, rights, and freedoms of the Data Subject;
		2. The processing is to establish, exercise, or defend a legal claim; and
		3. The processing is for scientific, historical, or statistical purposes carried out in the public interest (please note that this exemption is unlikely to apply to Taboola).
1. *Right to Restriction*

The Right to Restriction: This is a Data Subject’s right to require that Taboola restrict its processing of his or her Personal Data.

* 1. Where certain grounds are met (for example, where a Data Subject has contested the accuracy of data and a period of time is required for Taboola to verify the accuracy of the Personal Data or if Taboola is determining whether a Data Subject’s objection to processing overrides Taboola’s legitimate interests), the processing of the Data Subject’s Personal Data will need to cease, absent the Data Subject’s specific consent. If you believe you have received a request for restriction, please share it immediately with the Taboola Privacy Team, at privacy@taboola.com.
1. *Right to Data Portability*

The Right to Data Portability: This is Data Subject’s right to request that a controller provide any Personal Data that it processed with the Data Subject’s consent via automated means to another controller in a structured, commonly used, and machine-readable format.

* 1. For Taboola, this is likely to only apply when a Taboolar leaves Taboola to another employer. In such cases, Taboola shall take confidentiality into consideration before making any such transfer.
1. *Right to Not Be Subject to Automated Decision Making (Including Profiling)*

The Right to Not Be Subject to Automated Decision Making: This is the Data Subject’s right to object to an automated decision made about an individual (for example, without a human involved) which has a legal or other similar effect on the individual. Individuals can ask for human intervention in the process.

* 1. Taboola does not engage in this type of automated decision making.
1. *Right to Object to Direct Marketing*

The Right to Object to Direct Marketing: This is a Data Subject’s right to object to direct marketing, including profiling relating to direct marketing.

* 1. If Taboola receives a request to stop using Personal Data for direct marketing purposes, we must stop doing so. Please refer our Customers to [our subscription center](https://pages.taboola.com/SubscriptionCenter-with-Email.html) if you receive any such request and refer the request to the Taboola Privacy Team at privacy@taboola.com and Taboola’s Marketing Team at marketing@taboola.com.

# PRC Data Subject Rights Handling Policy

1. *Introduction*

Taboola has issued this PRC Data Subject Rights Handling Policy to describe the practices and procedures that Taboola follows when it receives requests about our use of Personal Data (in this PRC Policy, referred to as “Personal Information”) from: (i) individuals who interact with Taboola’s Content Distribution Platform (“Users”); (ii) publishers, advertisers, and other content providers with whom Taboola has a contractual relationship, ("Customers"); and (iii) Taboola’s permanent and non-permanent employees, former employees, contractors, consultants, temporary workers, interns, and volunteers ("Taboolars"). Any individual User, Customer, or Taboolar in the People’s Republic of China, (“PRC”) whose data is processed by Taboola shall each be referred to hereinafter as a “Data Subject”.

1. *Rights That All Data Subjects Have Regarding Their Personal Information*

Data Subjects have data protection rights that they may exercise by making a request to Taboola (a “Data Subject Rights Request”). These data subject rights include the:

* + - Right to be informed
		- Right to determine, restrict, and refuse data handling
		- Right to access and request a copy
		- Right to rectify and supplement
		- Right to delete
		- Right of portability
		- Right relating to automated decisions
		- Right of the deceased
	1. Each of these rights is described in more detail in [Sections 10-17 below](#bookmark=id.lnxbz9).
	2. The procedures described in this PRC Data Subject Rights Handling Policy outline how Taboola, as a processing entity (the entity determining the purpose for which, and manner in which, the Personal Information is processed), will respond to any Data Subject Rights Requests.
1. *Responsibility to Respond to a Data Subject Rights Request*
	1. The personal information processing entity of a Data Subject’s Personal Information is primarily responsible for responding to a Data Subject Rights Request and for facilitating the Data Subject’s exercise of his or her rights under applicable data protection laws. For example, because Taboola determines what data it will collect from its Taboolars, and how it will process this Taboolar data, Taboola is the processing entity of the Taboolar’s Personal Information that it holds and processes. As the processing entity of the Taboolar’s Data, Taboola must respond to any Data Subject Rights Request we receive from a Taboolar.
	2. In certain circumstances, Taboola may process a Data Subject’s Personal Information as an entrusted party on behalf of a third party who is the processing entity (rather than for its own purposes). In such instances, Taboola must inform the relevant third party promptly and provide it with reasonable assistance to help the third party honor the Data Subject’s rights in accordance with applicable data protection laws.
2. *Personal Information That Taboola Has Made Available to Third Parties*
	1. If Taboola shares Personal Information with third parties, it is our responsibility to inform those third parties of any request we receive from Data Subjects to rectify, erase, or restrict their Personal Information, unless doing so would involve disproportionate effort or is impossible. For example, when Taboola receives a Data Subject Rights Request, we must notify any relevant Taboola entity, processors, or other third parties (such as occupational health providers) that we have disclosed the Personal Information to, so that they may also update their records accordingly. As a general rule, in order to comply with this requirement, Taboola requires that all of its entrusted parties erase any Personal Information they receive from Taboola within thirty (30) days of their receipt of such Personal Information. If you have concerns about any service providers that you are engaged with, please consult with Taboola’s Legal Team, at legal@taboola.com. All Data Subject Rights Requests and questions that you receive from non-Taboolars should be sent to Taboola’s Privacy Team at privacy@taboola.com.
	2. If requested, Taboola must also provide the Data Subject with details about third parties to whom we have disclosed the Data Subject's Personal Information.
3. *Where Can You Send Your Own Data Subject Rights Requests and Questions?*
	1. If you are a Taboolar in the PRC, and you wish to make a Data Subject Rights Request regarding the Personal Information that Taboola holds about you, please send your request to privacy@taboola.com.
	2. Any questions regarding Taboolar Data Subject Rights Requests should also be sent to privacy@taboola.com.
	3. Users who engage with the Taboola Content Discovery Platform can make a Data Subject Rights Request via [Taboola's Global Data Subject Access Request Portal](https://accessrequest.taboola.com/access). All Data Subject Rights Requests and questions that you receive from non-Taboolars should be sent to Taboola’s Privacy Team at privacy@taboola.com.
4. *What to Do if You Receive a Data Subject Rights Request from a Taboolar or a Non-Taboolar Data Subject*
	1. If you receive a Data Subject Rights Request from another Taboolar, you should immediately direct the request to privacy@taboola.com. Please also include the date on which you received it, along with any other information that may help us efficiently respond to the request.
	2. If you receive a Data Subject Rights Request from a User who interacts with the Taboola Content Discovery Platform or from a Customer about a User request, you should (1) immediately refer the Data Subject to Taboola’s Data Subject Access Request Portal, available [here](https://accessrequest.taboola.com/access) and (2) immediately forward the request to Taboola’s Privacy Team, at privacy@taboola.com, and please also include the date on which you received it, along with any other information that may help us efficiently respond to the request.
	3. If you receive a Data Subject Rights Request about a Customer account, you should immediately direct the request to Taboola’s Privacy Team, at privacy@taboola.com. Please also include the date on which you received it, along with any other information that may help us efficiently respond to the request.
	4. PRC data protection legislation demands that Taboola respond to requests within a very short time frame, so it is crucial that you immediately direct any Data Rights Requests you receive to the appropriate person indicated above without delay.
5. *Verification Process*
	1. Taboola’s Privacy Team will assess every Data Rights Request that we receive to determine whether Taboola is the processing entity or an entrusted party of the data requested. We may also need to verify that the request has been made by a genuine Data Subject (which may require that we request further identification of the requestor).
	2. If we determine that Taboola is an entrusted party of the Data Subject’s requested data, and that one of Taboola’s Customers or another third party is the processing entity of this data, then Taboola shall notify the Customer or third party as soon as possible, per data protection regulations. Taboola shall also help the processing entity comply with the Data Subject Rights Request (in accordance with any contract terms which may be in place with the processing entity).
	3. If we determine that Taboola is the processing entity of the Data Subject’s requested data, Taboola shall contact the individual in writing to confirm receipt of the Data Subject Rights Request and seek confirmation of identity (if not already validated).
	4. If Taboola is not exempt under applicable data protection laws from fulfilling the Data Subject Rights Request (see Section 8.1, below), then Taboola, to the extent it deems necessary, will request any further information needed to action the individual's request. Once Taboola has all the information it needs to honor the Data Subject Rights Request, Taboola will respond to the request in accordance with Section 9, below.
6. *Exemptions from Requirement to Respond to a Data Subject Rights Request*
	1. If Taboola is exempt from the requirement to fulfill a received Data Subject Rights Request, then Taboola will notify the individual that we intend to decline the Data Subject Rights Request and explain why an exemption applies. Taboolars should always forward inquiries to Taboola’s Privacy Team, at privacy@taboola.com, who can make an assessment about whether such an exemption applies. Please never make this determination yourself.
7. *Timeframe for Responding to a Data Subject Rights Request*
	1. Data Subject Rights Requests must be responded to without undue delay It is imperative that you direct any requests that you receive immediately to Taboola Privacy Team, at privacy@taboola.com.
8. *Right To Be Informed*
	1. Data subjects have the right to be informed of the processing activities. In particular, the PIPL requires that processing entities should provide the following information to Data Subjects prior to the processing of their personal information:
		* 1. The identity and contact details of the processing entity;
			2. The purposes and methods of the processing;
			3. The type of Personal Information to be handled and the storage period;
			4. The methods and procedures for data subjects to exercise their rights;
			5. Other information that is required to be informed by laws and regulations; and
			6. Changes to the above, if any.
	2. If the above information is provided through privacy policies, such policies should be made public and easy to be accessed and saved. Data subjects have the right to request explanations on such policies.
	3. Applicable privacy law and regulations outline two instances in which a controlling entity will be exempted from the above obligations: where law or regulation requires that processing Personal Information be (1) confidential or (2) exempted from notification.
9. *Right To Determine, Restrict, and Refuse Data Processing*
	1. Data Subjects have the right to determine whether to permit the processing activities proposed by data handlers, and have the right to restrict or refuse whole or part of such activities.
	2. However, it is pending further clarification by PRC legislators as to how could a data subject exercise such rights (particularly for the circumstances where the data processing activities are relying on legal bases other than consent).
10. *Right Of Access And Right To Request A Copy Of Personal Information*
	1. Data subjects have the right to access and request a copy of their personal information, whilst the PIPL provides exceptions to such rights where law or regulation requires the processing of Personal Information (either carried out by government authorities or other data handlers) to be confidential or be exempted from notification.
11. *Right To Rectify And Supplement*
	1. Where the personal information is not accurate or complete, data subjects have the right to request data handlers to rectify or supplement the information in a timely manner (after necessary verification by data handlers).
12. *Right To Delete*
	1. Data subjects have the right to request the deletion of their personal information, under the circumstances that data handlers fail to delete the information after one or more of following circumstances is triggered:
		* 1. The purposes of data handling have been achieved, or have failed to be achieved, or it is no longer necessary for achieving the purposes;
			2. The processing entity has ceased to provide the products or services, or the agreed storage period has expired;
			3. Data Subjects have withdrawn their consent;
			4. The processing entity has violated applicable laws or regulations or any agreement relating to the handling of personal information; or
			5. Other situations provided for by law or regulation.
	2. Notably, if the statutory storage period is not expired (which may under other applicable laws and regulations) or it is technically unfeasible to delete the personal information, data handlers should cease the handling activities (except for taking necessary security measures and storage of information).
13. *Right Of Portability*
	1. As an important change brought by the PIPL, data subjects are granted the right to request their personal information to be transferred to other designated data handlers, provided that such request satisfies certain conditions to be raised by Cyberspace Administration of China ('CAC').
	2. However, the details on exercising such right are pending further clarification. Particularly, the CAC conditions are yet to be released to the public and it is also unclear as to the scope of personal information that could be portable.
14. *Right Relating to Automated Decisions*
	1. Where the personal information is used for automated decision and such decision may cause material impact to personal rights and interests, data subjects have the right to request an explanation on such handling activity and refuse to accept any determination that is made merely relying on the automated decision.
	2. Similarly, if the automated decision is applied for message pushes or marketing promotion, data subjects have the right to refuse such handling.
15. *Right Of The Deceased*
	1. For the Personal Information of the deceased, the above rights to access, copy, rectify, and deletion could be exercised by his/her close relatives (for lawful and legitimate interests of their own), unless there exists other arrangement that is priorly made by the deceased.