INTERNATIONAL TRADE CONTROLS COMPLIANCE POLICY

Last revised on March 28, 2023

This International Trade Controls Compliance Policy includes the following:

1. *Introduction*

Taboola.com, Ltd. and its affiliates and subsidiaries (collectively, "Taboola") are committed to promoting the highest standards of ethical business conduct. As part of this commitment, it is Taboola's policy to comply with all applicable laws, rules, and regulations.

As a global company, Taboola does business with people and companies around the world and must comply with all applicable export controls, economic sanctions, and antiboycott measures of, among others, the United States, Israel, the European Union and its Member States, and the United Kingdom (collectively, "Trade Control Laws"). All Taboola employees, officers, directors, contractors, and agents globally are required to comply with the Trade Control Laws, this International Trade Controls Compliance Policy, and any procedures developed by management to implement this Policy.

The purpose of this Policy is to educate Taboola personnel on Trade Control Laws and assist such personnel in complying with the letter and spirit of all applicable Trade Control Laws. Compliance with this Policy and all Trade Control Laws is mandatory. Violations of

the relevant laws or this Policy may lead to disciplinary action, up to and including termination of employment.

2. *Export Control Summary*

2.1 KEY EXPORT CONTROL PROVISIONS

Goods, software, software code, and technology/technical data (collectively, "Items") may be regulated for export control purposes, depending on the controls applicable to the Item and its destination, end use, and end user. One important consideration in assessing how these controls apply is how the Item is classified under export control laws. An Item's classification depends on its technical characteristics and whether and to what extent it is considered by government authorities to be sensitive for national security or other reasons. Notably, many jurisdictions classify under their respective export controls laws Items that use, incorporate, or call upon encryption functionality. Ensuring that Items are classified correctly for export controls purposes is critical to export controls compliance.

Taboola possesses certain Items, including software and software code, that are subject to heightened export controls restrictions. The Company verifies and maintains records of the export classification of these items. If you need any information on those export classification records or have questions on this, please reach out to the Taboola Legal Team.

(a) Scope and Application of U.S. Export Controls

The U.S. Export Administration Regulations ("**EAR**"), which are administered by the U.S. Department of Commerce, Bureau of Industry and Security ("BIS"), control exports, reexports, and in-country transfers outside the United States of commercial, some military, and dual-use Items (i.e., Items with both civil and military, terrorism, or proliferation applications).[1] U.S. export controls apply not only to physical exports of Items from the United States to another country *but also to transfers, uploads, or downloads of software across borders, and transfers or disclosures, inside and outside of the United States, of technology or software source code to non-U.S. nationals*.

In addition to regulating the export of Items from or through the United States, the EAR also apply to the movement of items outside the United States (including exports, reexports, and transfers) if such Items are:

- U.S. origin;

[1] Export controls with respect to most military items are administered by the U.S. Department of State, Directorate of Defense Trade Controls, and certain sensitive nuclear equipment, materials, and technology are controlled by the U.S. Department of Energy and the Nuclear Regulatory Commission. Because the Company's business does not involve items or activities regulated under these authorities, they are not addressed further herein.

- Manufactured or developed abroad but incorporate more than *de minimis* controlled U.S.-origin content (generally 10 or 25 percent controlled U.S.-origin content by value, depending on the destination to which the non-U.S. Item will be sent); or
- Manufactured abroad as the direct product of U.S.-origin technology or software that is controlled for national security reasons, or are produced by a plant that is the direct product of such controlled technology or software.

The concept of "U.S. origin" is applied broadly under the EAR. It generally includes any Item developed or modified within the United States. Additionally, any Item that is located in the United States, even if such Item is merely passing through the United States, is subject to control under the EAR at the point of its export from the United States. For example, cross-border transfers, uploads, or downloads of software or technical data from servers located in the United States would be subject to the EAR, including remote access from outside the United States to such technology/technical data or software source code if resident on a U.S.-based server.

These extraterritorial controls can be particularly important for companies such as Taboola that have many non-U.S. locations to which they may send technology, software, source code, or hardware, including for incorporation into non-U.S. Items. Importantly, both U.S. and non-U.S. persons/companies must comply with the EAR whenever they are exporting, reexporting, or transferring Items that are subject to the EAR.

Below, we discuss in more detail several aspects of the EAR that are relevant to Taboola. Please reach out to the Taboola Legal Team if you have any questions regarding these aspects.

(i) Deemed Exports and Deemed Reexports

In addition to restricting transfers of controlled Items from the United States to other countries and between non-U.S. locations, the EAR define "export" to include the release or disclosure of technology or software source code to a non-U.S. person in the United States. This is known as a "deemed export." A non-U.S. person is someone who is not a U.S. citizen or U.S. lawful permanent resident (i.e., a "green-card" holder), even if the person is legally employed in the United States. For example, a disclosure of software source code or technology in the United States to a national of Israel is "deemed" to be an export to Israel.

The EAR also govern "deemed reexports," which are releases or disclosures of U.S.-origin technology or software source code in one non-U.S. country to a national of a different non-U.S. country. For example, a disclosure of U.S.-origin software source code or technology in Israel to

an Indian national would be deemed to be a reexport of such source code to India.

Deemed exports or deemed reexports of technology and software source code can occur in a number of different ways, including, for example, through visual inspection by a non-U.S. person of U.S.-regulated technology or software source code in the United States or abroad.

(ii) Restricted Parties

Among other restrictions in the EAR, the EAR also broadly prohibit both U.S. and non-U.S. persons/companies from providing Items subject to the EAR to parties that are on certain lists administered by BIS. These include the Entity List and Denied Persons List. Both lists have targeted a number of parties around the world that present U.S. national security or foreign policy concerns (the focus of the Entity List) or that have violated U.S. law (the focus of the Denied Persons List).

Under the EAR, certain items intended for military end-users or military end-uses in Belarus, Burma, Cambodia, China, Russia, or Venezuela are subject to additional licensing requirements beyond those that normally apply to exports to those destinations. BIS has published a list of Military End Users subject to these restrictions, but it is not exhaustive, and the licensing requirements apply any time there is knowledge that an export, reexport, or transfer is intended for a military end-user or end-use in those countries.

Additional details on how Taboola conducts screening against applicable lists of sanctioned or restricted parties are provided in Section 3, below.

(iii) Embargoed Destinations

Export controls restrictions administered by BIS broadly restrict the export, reexport, or transfer of items subject to the EAR to countries and territories that are subject to U.S. comprehensive sanctions (currently Cuba, Iran, North Korea, Syria, and the Crimea, Donetsk People's Republic, and Luhansk People's Republic). Additional details on U.S. sanctions requirements are provided in Section 3, below.

Additionally, many, but not all, items subject to the EAR now require a license for export, reexport, or transfer to Belarus or Russia. Any potential exports, reexports, or transfers to these destinations (including deemed exports to nationals of these countries or territories) should be raised to the Taboola Legal Team.

(iv) Authorization, Reporting, and Recordkeeping

Whenever we seek to export, reexport, or otherwise transfer Items across borders, we must consider how the Item is classified for export control purposes and the destination, end use, and end user of the item. All these factors help us determine whether any government licensing or other authorization (such as reliance on a license exception) is needed, which must be determined – with any necessary authorization obtained – before the export, reexport, or transfer occurs.

In some cases, we may need to file reports with U.S. authorities about encryption-related products that are available on a mass-market basis, and we may also need to file – in the case of tangible exports – export-related information with the U.S. Census Bureau for export control and tracking purposes. In addition, we should maintain export-related records for a period of at least five years.

(b) Scope and Application of EU Export Controls

Export controls in the European Union are regulated under the Recast EU Dual Use Regulation, which is directly applicable in all 27 EU Member States. The Recast Dual Use Regulation controls many of the same types of goods, software, and technology as the U.S. EAR — the two regimes derive, in large part, from international treaties and export controls arrangements to which both the United States and EU are parties. As with the case of the U.S. EAR, the Recast Dual Use Regulation controls both physical exports as well as *intangible* exports of software or technology, such as through uploads/downloads of software, other electronic transfers, or discussions that result in the conferral of restricted technical information.

In contrast to the U.S. EAR, the Recast Dual Use Regulation generally does *not* impose "deemed export" controls, or broad controls on the overseas transfer of EU-origin items. The Recast Dual Use Regulation is likely to be most relevant for Taboola in two ways:

- First, Taboola could face EU export licensing requirements if it were, from locations within the EU, to transfer restricted goods, software, or technology to persons located outside the EU, or to persons within the EU with knowledge that those persons intended to remove the restricted items from the EU without a license.

- Second, if Taboola were to receive restricted goods, software, or technology outside of the EU from EU suppliers, Taboola might be required to sign "end user undertakings" with those EU suppliers that impose restrictions on Taboola's ability to retransfer those items to other persons or locations.

(c) Scope and Application of United Kingdom Export Controls

United Kingdom export controls restrict the transfer of sensitive goods, software, information and technology to persons located outside of the United Kingdom. This includes physical exports, electronic transfers, and transfers by any other means, such as verbal communication. Items that are subject to export controls are consolidated and listed within the UK Strategic Export Control Lists. The UK Strategic Export Controls Lists include not only military and dual-use listed Items, but also torture equipment, non-military firearms and radioactive sources – none of them applied to Taboola.

If an item intended for export is referenced on the UK Strategic Export Control Lists, it will be necessary to apply for a licence from the Export Control Joint Unit ("ECJU"). The ECJU has the power to invoke "end-use controls" even where an item is not listed on the UK Strategic Export Controls Lists if there are any specific concerns about military or weapons of mass destruction end-use.

The United Kingdom's export control regime is substantially aligned with the EU as both derive from the same international standards. However, as the United Kingdom is no longer a member state of the EU, shipments of dual-use items to the EU from the United Kingdom will require export authorisation, subject to available licences.

(d) Scope and Application of Israeli Export Controls

(i) Import and Export Order (Control of Dual- Purpose Use Goods, Services and Technology Exports), 2006

- The Wassenaar Arrangement is an export control regime regarding conventional arms and dual-use goods and technologies.
- Israel is not a party to the Wassenaar Arrangement. Yet, according to the Import and Export Order (Control of Dual- Purpose Use Goods, Services and Technology Exports), 2006, in order to export a product which is on the Wassenaar Dual-Use List, Taboola must have an export license from the Israeli Ministry of Economy and Industry.

(ii) Order Governing the Control of Commodities and Services (Engagement in Encryption Items), 1974

- In Israel, the State regulates use of encryption items through the Order Governing the Control of Commodities and Services (Engagement in Encryption Items), 1974.

- An export license for encryption items will be granted after scrutiny by the Israeli Ministry of Defense, and the license has to be renewed annually.
- Taboola will be exempted from applying for a license for engagement in commercial encryption items in any of the following cases:
    - The encryption item was purchased from a license holder for sale and distribution of such item.
    - The encryption item was "downloaded" from the Internet for Taboola's personal use for data security or electronic signature purposes.

2.2 PENALTIES FOR VIOLATIONS

The U.S. government may impose substantial civil monetary penalties for export violations, including penalties under the EAR of approximately $330,000 per violation or twice the value of the transaction, whichever is greater.[2] Criminal penalties with even larger fines and potential jail time also are possible for willful violations, and can be imposed on companies or individuals. In severe cases, the U.S. government also can debar the party that has committed the violation or deny its ability to export or receive U.S. items.

In the EU, penalties are imposed by the individual EU Member State authorities, and the ranges of potential civil and criminal penalties that can be imposed vary by Member State. Penalties can, however, be significant, and the EU authorities also can respond to violations in other ways that could have an adverse impact on Taboola's business, such as by restricting the ability of Taboola to receive export licenses, or to receive certain types of restricted items from EU suppliers.

In the United Kingdom, breaching export controls is a criminal offence. Penalties vary depending on the nature of the offence. They can include revocation of a license, seizure of goods, issuing a compound penalty fine and imprisonment for up to 10 years.

In Israel, violation of the 1939 Trading with the Enemy Ordinance may lead to a criminal penalties of fines or imprisonment, up to ten years.

3. *Economic Sanctions Summary*

3.1 TYPES OF SANCTIONS

Many countries – including the United States, European Union and its Member States, United Kingdom, and Israel – have enacted economic sanctions measures targeting trade

[2] Civil penalty amounts are adjusted annually for inflation.

with certain countries, territories, individuals, and entities. Sanctions change frequently in response to world events. The description below is current as of the date of this Policy, but you should consult with the Taboola Legal Team (legal-sanctions@taboola.com) for the most up to date information.

Generally, there are three types of primary sanctions:

(a) Comprehensive Country/Territory-Based Sanctions

Cuba, Iran, Syria, and North Korea are subject to comprehensive U.S. sanctions, which are primarily administered by the U.S. Department of the Treasury, Office of Foreign Assets Control ("OFAC"). Additionally, the Crimea, so-called Donetsk People's Republic, and so-called Luhansk People's Republic regions of Ukraine is subject to comprehensive sanctions imposed by the United States. Virtually all directly or indirectly transactions or dealings with, including campaigns that specifically target those, countries or territories that are subject to these sanctions, as well as with their governments, entities, and residents, are prohibited.

Both the European Union and United Kingdom maintain very broad sanctions regimes with regard to several countries and territories, including Crimea, so - called Donetsk People's Republic, the so- called Luhansk People's Republic, Iran, North Korea, and Syria. While not as comprehensive as the U.S. sanctions noted above, these EU and UK sanctions could potentially affect Taboola's business activities in a number of ways should it conduct business in, or with persons or entities who are established in, the foregoing countries/territories.

In Israel, the 1939 Trading with the Enemy Ordinance categorically and comprehensively bans all forms of trade, directly and indirectly, with Iran, Iraq, Syria, and Lebanon.

(b) Property-Blocking Sanctions

The EU, UK and the United States have imposed property-blocking sanctions on sanctioned/designated entities and persons in various countries that are listed on sanctioned party lists. U.S. and/or EU and/or UK persons are prohibited from engaging in virtually any transactions or dealings with or for the benefit of sanctioned/designated parties or with any entities owned 50 percent or more by or, in the case of the EU and UK, controlled by, one or more designated parties, unless licensed by the relevant authority. Such sanctions also require that the property and interests in property of all such parties be blocked (i.e., frozen) when such property or interests in property come into the United States (or the EU or UK) or the possession or control of a U.S. and/or EU person and/or UK person. Relatedly, the U.S. government also has imposed broad property-blocking sanctions on the Government of Venezuela, and entities it owns or controls or those that act or have acted on its behalf.

(c) Sectoral Sanctions

The U.S., EU and UK have enacted targeted "sectoral" sanctions against designated persons/companies in the Russian financial, defense, and energy sectors. Examples of activities targeted by these sectoral sanctions include limitations on dealings in new debt, new equity, and financial instruments of some Russian financial institutions and their affiliates; restrictions on dealing in new debt of some Russian defense and energy concerns, as well as restrictions on U.S. person support for certain energy projects; and certain related U.S., EU and UK export control restrictions. The sectoral sanctions are set out in the United States in four OFAC directives, and apply not only to parties on the U.S. Sectoral Sanctions Identifications List ("SSI List") but also to entities that such persons own 50% or more. In response to Russia's 2022 invasion of Ukraine, the United States, EU, and UK have also imposed a number of additional sanctions targeting Russian financial institutions (including the Russian Central Bank), state-owned entities, sovereign debt, and exports and imports of certain goods or services to or from, and new investment in, Russia.

In addition, as noted above, Venezuela is targeted for a number of U.S. sanctions that are primarily focused on its government (as broadly defined) and which also include a restriction on dealing in Venezuelan cryptocurrencies.

In December 2022, the UK amended its Russia sanctions to extend the prohibition on provision of certain professional services to Russia or persons connected with Russia to include advertising services. As a result, Taboola Europe Ltd., Taboola's UK affiliate (and those employed by that entity) and all UK nationals working for any other Taboola entity are not authorized to sell/manage/operate accounts/vendors that fall under that scope. There isn't yet a lot of guidance on what "connected to Russia" means, so Taboola evaluates several factors to make that determination, such as location of the client/publisher/advertiser, location of the POCs, billing addresses, telephone numbers, targeted countries. If you come across an existing account that may fall within that scope or a lead you wish to pursue, please reach out to legal-sanctions@taboola.com.

(d) Military Trade Sanctions

The U.S., EU and UK also maintain military trade embargoes against a range of countries. Those sanctions restrict the provision, by U.S., EU or UK persons, of a range of goods and services to countries that are subject to arms embargoes. Israel maintains similar de-facto embargoes through limitations or cancellations on the licensing of export controlled items for export for such jurisdictions.

Dealings with any entity or individual located in or ultimately controlled by an individual located on the following countries/territories are strictly forbidden: Iran, Iraq, Lebanon,

Libya, North Korea, Syria, Cuba, as well as the Crimea, so-called Donetsk People's Republic, and so-called Luhansk People's Republic regions of Ukraine.

Furthermore, all accounts on Salesforce and vendors on Netsuite are automatically and constantly checked against applicable sanctions and restricted parties lists, including but not limited to those issued by the US, UK, EU, and Israel governments. In case your account or vendor is flagged, you will receive an email requesting you to wait for the Taboola Legal Team instructions before proceeding to sell, upsell, or in any way manage that account or engage that vendor. A detailed training is available on Bridge, and the entire organization, as well as all independent contractors are required to complete it.

3.2 LICENSES AND EXEMPTIONS

Certain otherwise prohibited transactions involving sanctioned countries, territories, or persons may be authorized by licenses issued by the relevant government authority. Such authorization may be in the form of a "general license" which is published and can be utilized by any person, subject to the terms and conditions of the license, or a "specific license," which is issued to a particular person upon application to the relevant authority. Under U.S. sanctions, certain types of transactions, including the importation or exportation of pre-existing information or informational materials, and transactions relating to travel, are exempt from the prohibitions of many sanctions programs. Any reliance on a license or exemption to conduct a transaction involving a sanctioned country, territory, or person requires prior consultation with, and approval by, the Taboola Legal Team.

3.3 RECORDKEEPING AND REPORTING

Persons holding blocked property are required to submit reports to the relevant government authority, and with respect to U.S. sanctions, reporting is also required for transactions that are rejected due to sanctions prohibitions. In addition, we should maintain records relating to transactions involving sanctioned countries/territories/persons for a period of at least five years.

3.4 PENALTIES FOR VIOLATIONS

The U.S. government may impose substantial civil monetary penalties for primary sanctions violations. Violations of most of the primary sanctions are subject to maximum civil penalties of approximately $330,000 per violation, or twice the value of the transaction, whichever is greater.[3] Criminal penalties with even larger fines and/or jail time also can be imposed on entities or individuals for willful violations.

In the EU, as with the Recast Dual Use Regulation penalties for violations of sanctions regulations differ among the EU Member States. The potential penalties are, however,

[3] Civil penalty amounts are adjusted annually for inflation.

generally very significant, and include both civil and well as criminal penalties (including monetary fines and, in the case of criminal violations, possible jail time).

In the UK, breaches of financial sanctions are treated as a serious criminal offence. Offences relating to the principal prohibitions under UK financial sanctions carry a maximum of 7 years' imprisonment. The Office for Financial Sanctions Implementation has the power to impose monetary penalties ranging from 50% of the estimated value of the funds or economic resources relating to the breach or £1 million, whichever is the greater value. Reduced monetary penalties are available in relation to cases that have been voluntarily disclosed to OFSI.

4. *Antiboycott Summary*

U.S. antiboycott laws prohibit Taboola and its subsidiaries from engaging in activities that support international boycotts opposed by the United States, such as the Arab League boycott of Israel. Agreeing to engage in such activities also could expose Taboola to adverse tax consequences under the antiboycott measures in the U.S. tax code. Such activities may include, for example, refusing to do business with a party in a boycotted country or a party included on a "blocklist" for doing business with a boycotted country, or entering into contracts or agreements that provide that Taboola will not do business with a boycotted country or blocklisted party or will comply with the laws of a boycotting country.

These laws also require reporting to the U.S. government (either the U.S. Commerce Department or the U.S. Treasury Department or both) the receipt of a request to engage in boycott-related activities, even if Taboola does not respond or agree to the request.

Boycott-related requests can come in any form, written or oral, and may appear in such documents as requests for proposal, bid or tender invitations, proposed contracts, purchase orders, invoices, or letters of credit. Boycott-related requests are particularly likely to come from the following countries, which are currently identified by the U.S. government as boycotting countries:

- Iraq
- Kuwait
- Lebanon
- Libya
- Qatar
- Saudi Arabia
- Syria
- Yemen

Boycott-related requests also may come from other countries, including Bahrain, Bangladesh, Malaysia, Oman, and Pakistan.

When reviewing transaction documentation, you must be alert for suspected boycott-related requests. If you identify a suspected boycott-related request, you may not accept or otherwise respond to the request, and must immediately report the request to the Taboola Legal Team. The Taboola Legal Team will review the request to determine whether reporting is required under U.S. antiboycott laws, and will provide guidance as to whether the request must be removed from the contract or other document in which it appears, amended, or other action taken.

In the EU, a number of antiboycott measures are in place that restrict, in certain respects, EU persons from complying with foreign sanctions laws. For instance, the EU has in place what is known as the EU Blocking Regulation, which restricts EU persons from complying with aspects of the U.S. sanctions against Iran and Cuba. A separate measure is in place in Germany that restricts German nationals from complying with certain foreign sanctions. In the United Kingdom, the EU Blocking Regulation has been incorporated into domestic law following the UK's withdrawal from the EU. As a result, UK persons are also restricted from complying with aspects of U.S. sanctions applicable to Iran and Cuba. The requirements set forth in this policy are consistent with the EU and UK antiboycott regulations, as Taboola's international sanctions compliance posture is motivated by aspects of U.S. and international sanctions that are not prohibited under EU and UK law. To the extent any Taboola personnel receive inquiries concerning the EU or UK antiboycott/blocking regulations, please consult with the Taboola Legal Team.

5. *Red Flags*

Taboola employees and independent contractors are expected to say something when they see something. If an employee or independent contractor sees "red flags" or other circumstances that suggest a potential violation of this Policy or any applicable law, he or she must not turn a blind eye. If an employee or independent contractor sees something that suggests someone at Taboola or one of its agents might be acting in violation of this Policy, he or she should immediately contact his or her supervisor or the Taboola Legal Team.

While conducting Taboola business, employees and independent contractors must monitor for any "red flags." A red flag is an abnormal circumstance in a transaction that indicates that an export may be destined for an unauthorized end use, end user, or destination. Red flags may appear in many forms and can include:

- The publisher, OEM, carrier, utility, app, distribution partner, content provider ("Partner")/Advertiser or its address is similar to one of the parties found on the U.S. Commerce Department's Denied Persons or Entity Lists;
- The Partner/Advertiser is reluctant to offer information about the end use or end user of the Item;

- The Item's capabilities do not fit the Partner/Advertiser's line of business;
- The Item is incompatible with the technical level of the country to which it is being provided;
- The Partner/Advertiser is willing to pay cash for a very expensive Item when the situation would normally call for financing;
- The Partner/Advertiser has little or no business background;
- The Partner/Advertiser is unfamiliar with the product's performance characteristics but still wants the product; or
- When questioned, the Partner/Advertiser is evasive and unclear about whether the purchased product is for domestic use, export, or reexport.

In short, a "red flag" is anything that is out of the ordinary and does not appear above-board. Each employee and independent contractor is responsible for monitoring his or her email and other communications for red flags. Any red flags should be brought promptly to the attention of the employee's or independent contractor's supervisor or the Taboola Legal Team. Failure to do so is considered a violation of this Policy.

6. *Reporting Violations of this Policy*

No policy can anticipate every situation that may arise. Accordingly, this Policy is not meant to be all-inclusive, but rather it is intended to serve as a source of guiding principles and to encourage communications concerning the standards of conduct addressed in this Policy. Employees and contractors are encouraged to reach out to the Taboola Legal Team (legal-sanctions@taboola.com) with questions about particular circumstances that may implicate the provisions of this Policy.

Compliance with this Policy is, first and foremost, the individual responsibility of every Taboola employee and independent contractor. It is the individual responsibility of each Taboola employee and independent contractor whose duties are likely to lead to involvement in or exposure to any of the areas covered by the Trade Control Laws and regulations of the jurisdictions in which Taboola operates, by action and supervision as well as continuous review, to ensure strict compliance with this Policy.

Any Taboola employee or independent contractor who suspects or becomes aware of any violation of this Policy or any Trade Control Laws shall report the violation to his or her supervisor, who will immediately inform the Taboola Legal Team (legal-sanctions@taboola.com), who shall coordinate an investigation into the reported matter. The Taboola Legal Team shall communicate the results of any such investigation directly to the Finance Department and the CEO and, if necessary, to the Company's Board of Directors. Taboola may take severe disciplinary action, up to and including dismissal, against any employee who violates this Policy. Awareness of and failure to report a violation or possible violation may lead to disciplinary action as well. It is against Taboola's labor

and employment policy to retaliate against any employee for making a good-faith report of a potential violation related to this Policy or any law.

7. *Certification*

From time to time, Taboola employees and independent contractors may be required to complete international trade controls compliance training and sign a certification acknowledging commitment to, full understanding of, and compliance with this Policy.

8. *Risk Assessment and Review*

The Taboola Legal Team will as appropriate conduct Sanctions and export control risk assessments that include an assessment of the following: (i) customers, supply chain, intermediaries, and counter-parties; (ii) the products and services it offers, including how and where such items fit into other financial or commercial products, services, networks, or systems; and (iii) the geographic locations of the organization, as well as its customers, supply chain, intermediaries, and counter-parties. Taboola will update the Policy as appropriate, taking into account the results of such risk assessments.

Taboola will periodically review the implementation of the Policy and the Company's internal controls to prevent violations of applicable sanctions and export controls requirements, which may as appropriate include reviews of the policy as part of internal audits. Results of such reviews, including any issues identified and remedial steps taken, will be provided to the Finance Department and the COO and, if necessary, to the Company's Board of Directors.

9. *Revision History*

Date of Change	Responsible	Summary of Change
----	----	----