The Trade Desk

Data Transfer Impact Assessment

Abstract

The Trade Desk is committed to enabling clients to use The Trade Desk platform services in compliance with the EU's data protection regulations, including the General Data Protection Regulation (GDPR). This document provides information about our services as well as resources to help clients conduct data transfer assessments in light of the "Schrems II" ruling about transfers of personal data subject to GDPR, and subsequent recommendations from the European Data Protection Board (EDPB). This document also describes the applicable measures taken by The Trade Desk to protect personal data.

Notice

Clients are responsible for making their own independent assessment of the information in this document. This document: (a) is for informational purposes only, (b) represents The Trade Desk's current product offerings and practices, which are subject to change without notice, and (c) does not create any commitments or assurances from The Trade Desk and its affiliates, suppliers or partners. The responsibilities and obligations of The Trade Desk to its clients are controlled by our agreements, and this document is not part of, nor does it modify, any agreement between The Trade Desk and its clients.

Background

The EU's new Standard Contractual Clauses (SCCs) address the consequences of Schrems II. Section III of the SCCs, entitled "Local Laws and Obligations in Case of Access by Public Authorities", requires parties to demonstrate that they have no reason to believe that the laws of the destination country will prevent compliance with the SCCs. In doing so, the data importer and the data exporter are asked under the new SCCs to conduct a documented assessment, typically referred to as a data transfer impact assessment (DTIA), into the specific circumstances of the transfer and the laws and practices of the destination country that are relevant in light of the specific circumstances of the transfer.

Further with respect to Schrems II, the EDPB released its (a) Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, and (b) Recommendations 02/2020 on the European Essential Guarantees for surveillance measures. When conducting a DTIA, the SCCs should be read together with these recommendations.

Overview of the EDPB Recommendations

The EDPB provided examples of supplementary measures in its "Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data"[1] (EDPB Recommendations). The EDPB Recommendations also provide guidance for assessing whether there is an essentially equivalent level of protection for data transfers outside the European Economic Area (EEA) following Schrems II. Data exporters are recommended to perform the following six-step data transfer assessment (the EDPB data transfer assessment):

- Step 1: Perform a mapping of international data transfers and assess whether the data transferred is adequate and limited to what is strictly necessary.
- Step 2: Verify the transfer tool on which the transfer relies (for example, the use of SCCs as the safeguarding mechanism to transfer personal data).
- Step 3: Assess the laws or practices of the third countries that may impinge on the effectiveness of the appropriate safeguards of the transfer tool, including by using Recommendations 02/2020 on the European Essential Guarantees for surveillance measures.
- Step 4: If the data exporter's assessment is that the use of the transfer tool alone would not provide an essentially equivalent level of protection, identify the supplemental contractual, technical or organizational measures that are necessary to bring the level of protection of the data transferred up to the EEA standard of essential equivalence.
- Step 5: Take any formal procedural steps the adoption of your supplementary measure(s) may require.
- Step 6: Re-evaluate, at appropriate intervals, the level of protection afforded to the data that the data exporter transfers to third countries and monitor if there have been or there will be any developments that may affect it.

[1] See https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en

Step 1: Identify International Data Transfers. Perform a mapping of international data transfers and assess whether the data transferred is adequate and limited to what is strictly necessary.

What is The Trade Desk Platform?

The Trade Desk offers what is known in the industry as a demand-side platform (the "Platform"). We provide technology that helps advertisers and their advertising agencies manage digital advertising campaigns across many channels, such as websites, apps, audio, smart TVs, and other video. The Platform is used to plan, forecast, execute and report on data-driven digital advertising campaigns across diverse ad formats. Our integrations with data, inventory and publisher partners provide ad buyers reach and decisioning capabilities, and our enterprise tools enable our clients to develop on top of the Platform. Learn more about our Platform here.

Purposes

In order to provide our products and services, The Trade Desk transfers limited types of personal data to the US for core data processing. We process personal data to effectively enable clients to manage digital advertising and purchase digital inventory for the purpose of displaying ads via real time bidding (RTB). RTB is a real time auction of advertising space on, i.e., a web-page, allowing marketers to run automated online campaigns with predefined advertisement values, such as attributes of a target audience – demography, interests or purchase intentions. To learn more about RTB, please visit the Internet Advertising Bureau's website.

We, and our clients, collect and use data in the RTB context to help ensure that the ads are relevant and to measure and report on their effectiveness, among other things. The personal data that the Platform processes is limited to pseudonymous online identifiers (i.e, cookie or device IDs). See our Privacy Policy for more details.

US Data Transfer

Through the Platform, clients have the capability to run and manage their advertising campaigns across global regions to extend their reach. As such, The Trade Desk necessarily maintains data centers in various locations to support global campaigns. Personal data is initially collected and stored in the region closest to the point of data collection (depending on where the campaign is run) and subsequently transferred to US. For example, EU data is initially hosted by data centers in EU and UK. Thereafter, data is transferred to the US for primary processing and storage. We do so under a valid legal framework, such as through the use of SCCs.

General Attributes and Transactional Flow

The organizational sources of personal data on the Platform comprise:

(i) Inventory partners
(ii) Third party data suppliers

(iii) Advertising clients

What happens in an RTB transaction?

Available publisher inventory is passed to the Platform through our integrations with supply sources. During client advertising campaigns, the Platform submits bids on inventory based on client criteria. For example, in a campaign setup, clients decide on the relevant audiences and configure specific details of their campaign on the Platform. Audiences may be based on the clients' own first party data or third party audience segments available on the Platform.

Thereafter, on receipt of a publisher bid request, the Platform determines the best creative(s) and advertiser(s) and appropriate bid price to send back as a bid response. If The Trade Desk's bid wins, then a call from the publisher ad server is routed to the advertiser ad server for the winning creative to be served. Upon the creative serving, a feedback mechanism informs the Platform that the impression has served. The below chart provides a general overview of each stage of processing.

Processing Activity	Description of key attributes
Bid Request {Flow: Supply Partner → Trade Desk}	pseudonymous identifiers (i.e., device identifier) and related details of impression (i.e., browser information). Bid requests conform with industry specifications. See "Bid Request" specification at IAB OpenRTB Specification.
Bid Response (based on client targeting parameters) {Flow: Trade Desk → Supply Partner}	bid price; bid request identifier. See "Bid Response" specification at IAB OpenRTB Specification.
Bid Won {Flow: Supply Partner → Trade Desk}	Similar data as in bid request.
Ad is Served {Flow: Advertising Client → Trade Desk}	creative identifier; advertiser identifier; cookie identifier; other data that may be optionally passed at the discretion of the client, i.e., via pixel (cannot be direct identifying data).
Bid Feedback Mechanism {Trade Desk}	transactional record (a subset of the above attributes).

Step 2: Verify the transfer tool on which the transfer relies (for example, customers rely on the SCCs to transfer customer data).

When transferring personal data to third countries that have not been deemed adequate by the European Commission, The Trade Desk relies on the SCCs (pursuant to Regulation (EU) 2016/679 of the European Parliament and the Council approved by European Commission Implementing Decision (EU) 2021/914 of 4 June 2021). The categories of personal data that may be transferred are the pseudonymous online identifiers described in Step 1 above. Please also refer to The Trade Desk's Privacy Policy.

Step 3: Assess the laws or practices of the third countries that may impinge on the effectiveness of the appropriate safeguards of the transfer tool, including by using Recommendations 02/2020 on the European Essential Guarantees for surveillance measures.

The Trade Desk recognizes that Schrems II has generated uncertainty about the impact of US surveillance laws on EU personal data transfers. To address these issues, we have set out specific information about certain US laws considered by the Court of Justice of the European Union (CJEU) ruling and their application to the Platform.

Transfers to the United States

The Schrems II ruling has focused European attention on the breadth of law enforcement powers, particularly with respect to national security programs that permit US government agencies to engage in proactive surveillance. The following US laws were identified by the CJEU as being potential obstacles to ensuring essentially equivalent protection for personal data in the US.

I. Executive Order 12333 ("EO 12333")

EO 12333 authorizes and governs surveillance activities by US intelligence agencies. As the CJEU noted, the primary concern regarding EO 12333 is the US government's ability to collect personal data while it is in transit to the US by intercepting data travelling over transatlantic cables. Personal data can effectively be protected from this type of interception through security measures such as encryption. We address this risk today by transferring data through encrypted channels. Please see below for more information about these measures.

It is important to note that EO 12333 does not grant the US government the ability to compel private companies (such as The Trade Desk) to provide assistance with the above activities. Moreover, The Trade Desk contractually commits to its clients that it will not do so voluntarily. As a result, The Trade Desk does not and cannot be ordered to take any action to facilitate the type of bulk surveillance under EO 12333 that was considered problematic in the Schrems II ruling. In the unlikely event that US intelligence agencies were interested in the type of data that the Platform processes, safeguards such as the requirement for authorization by an independent court and the necessity and proportionality requirements would protect data from excessive surveillance.

II. FISA Section 702

Section 702 of the Foreign Intelligence Surveillance Act ("FISA Section 702") sets forth processes and conditions for US intelligence agencies to lawfully collect information relating to non-US persons who are reasonably believed to be located outside the US if a significant purpose of such collection is to acquire foreign intelligence information and the source of the information is a US-based electronic communication service provider ("ECSPs"). FISA Section 702 authorizes "upstream" and "downstream" collection.

Upstream collection authorizes US authorities to collect communications as they travel over the internet backbone. The Trade Desk does not provide such backbone services, but only handles traffic involving our own clients. As a result, The Trade Desk is not eligible to receive the type of orders principally addressed in, and deemed problematic by, the Schrems II ruling.

Downstream collection authorizes US authorities to collect targeted data directly from ECSPs based in the US. If in the unlikely event that The Trade Desk may be compelled to respond to such a targeted request for client personal data, we will carefully review the request to verify it is lawful and challenge the request in accordance with The Trade Desk's policies and contractual commitments on government access requests.

U.S. Surveillance Whitepaper

More information on the surveillance program operated pursuant to the above laws can be found in the whitepaper from September 2020, issued in response to the Schrems II ruling. The whitepaper details the limits and safeguards pertaining to US public authority access to data – see U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II.

Regarding FISA 702 – the whitepaper notes:

- For most companies, the concerns about national security access to company data highlighted by Schrems II are "unlikely to arise because the data they handle is of no interest to the U.S. intelligence community."
- There is individual redress, including for EU citizens, for violations of FISA section 702 through measures not addressed by the court in the Schrems II ruling, including FISA provisions allowing private actions for compensatory and punitive damages.

Regarding Executive Order 12333 – the whitepaper notes:

- EO 12333 does not on its own "authorize the U.S. government to require any company or person to disclose data." Instead, EO 12333 must rely on a statute, such as FISA 702 to collect data.
- Bulk data collection, the type of data collection at issue in Schrems II, is expressly prohibited under EO 12333.

The Clarifying Lawful Overseas Use of Data (CLOUD) Act

For more information on the CLOUD Act, see the following whitepapers:

- Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act (US Department of Justice)
- What is the CLOUD Act? (BSA Software Alliance)

The whitepapers note:

- The CLOUD Act only permits U.S. government access to data in criminal investigations after obtaining a warrant approved by an independent court based on probable cause of a specific criminal act.
- The CLOUD Act does not allow U.S. government access in national security investigations, and it does not permit bulk surveillance

Based on the foregoing reasons, it is highly unlikely that The Trade Desk would be subject to the surveillance laws identified in Schrems II.

Step 4: Identify the supplemental contractual, technical or organizational measures that are necessary to bring the level of protection of the data transferred up to the EEA standard of essential equivalence (this step is only necessary if the assessment reveals that the third country legislation and/or practices impinge on the effectiveness of the Article 46 GDPR transfer tool (safeguard) relied upon in the context of the data transfer).

For the reasons described in this document, no additional supplementary measures are necessary at this time. Below is a summary of existing measures The Trade Desk currently has in place.

Technical Measures:

The Trade Desk provides the following technical measures to secure personal data:

- Encryption: data in transit encrypted to secure communications over the internet
- Data Obfuscation: truncation and hashing where appropriate
- Security: implementation of controls in accordance with industry security standards to restrict access and safeguard personal data on its systems

Contractual Measures:

Contractual measures are set out in The Trade Desk's Data Processing Addendum which incorporates the SCCs. In particular, we are subject to the following requirements:

- Technical measures: The Trade Desk is contractually obligated to have in place appropriate technical and organizational measures to safeguard personal data (under the Data Processing Addendum as well as the SCCs we enter into with clients and service providers).

- Transparency: The Trade Desk is obligated under the SCCs to notify its clients in the event it is made subject to a request for government access to client personal data from a government authority. In the event that we are legally prohibited from making such a disclosure, The Trade Desk is contractually obligated to challenge such prohibition and seek a waiver.
- Challenging access requests: Under the SCCs, The Trade Desk is obligated to review the legality of government authority access requests and challenge such requests where they are considered to be unlawful.

Organizational Measures:

The Trade Desk's organizational measures to secure personal data include:

- Policy for government access to data: Policy must be followed for any government requests for data (for example, to obtain data from The Trade Desk, law enforcement officials must provide legal process appropriate for the type of information sought, such as a subpoena, court order, or a warrant).
- Onward transfers: Whenever we share your data with service providers, we remain accountable for how it is used. The Trade Desk requires all service providers to undergo a thorough cross-functional diligence process by subject matter experts in our Security, Privacy, and Product Teams to ensure users' personal data receives adequate protection. This process includes a review of the data expected to be shared with the service provider and the associated level of risk, the vendor's security policies, measures, and third party audits, and whether the vendor has a mature privacy program that respects the rights of data subjects. The list of our sub-processors is available to existing clients on The Trade Desk's sub-processors page.
- Privacy by design: While The Trade Desk does not rely on the Privacy Shield framework for data transfers, we continue to live up to obligations under the program. The Trade Desk adheres to key principles that outline our approach to privacy. More detailed information available here.

Step 5: Take any formal procedural steps the adoption of your supplementary measure(s) may require.

In light of the information provided in this document, including The Trade Desk's existing technical, contractual, and organizational measures that have been implemented to protect client personal data, The Trade Desk considers that the risks involved in transferring and processing European personal data in/to the US do not impinge on our ability to comply with our obligations under the SCCs (as "data importer") or to ensure that individuals' rights remain protected. Therefore, no additional supplementary measures are necessary at this time.

Step 6: Re-evaluate, at appropriate intervals, the level of protection afforded to the data that the data exporter transfers to third countries and monitor if there have been or there will be any developments that may affect it.

The Trade Desk will review and, if necessary, reconsider the risks involved and the measures it has implemented to address changing data privacy regulations and risk environments associated with transfers of personal data outside of Europe.