mediaocean

Transfer Impact Assessment

PLATFORM AND SERVICES | CLIENT SUMMARY

Document control

Date	25 Mar 2024
Author	Alex Krylov (Lucid Privacy Group)
Reviewed by	Ola Grela, Director, Compliance & Audit
Review Date	11 Apr 2024

Introduction

Under the European data protection laws, personal data may not be transferred outside of Europe unless (i) the importing country has been deemed adequate by the relevant governmental body; or (ii) the data exporter has appropriate safeguards in place to ensure that personal data transferred is subject to an adequate level of protection. Those safeguards are referred to as “transfer mechanisms.” The information below details the transfers and transfer mechanisms applicable to

- This **Transfer Impact Assessment** (“TIA”) assists Mediaocean (“we”, “us”, “our”) clients and partners in conducting a risk assessment for the transfer of personal data in connection with Mediaocean’s provision of its services (including advertising infrastructure and ad serving products).
- **Related information** about the third party vendors and suppliers Mediaocean uses, please visit our sub-processor page, company privacy policy, regional hosted systems privacy policies (US, EMEA, APAC), Data Protection Addendum and EEA Standard Contractual Clauses.
- **Further information** may be accessed through our Legal & Compliance portal**.**

Scope

This TIA addresses the processing (including transfer) of such personal data by Mediaocean, its affiliates and sub-processors in light of the “Schrems II” ruling of the Court of Justice for the European Union and the recommendations from the European Data Protection Board. It provides information necessary to comply with personal data transfer rules under European data protection law.

- **Types of data transfers:** The TIA covers direct and onward data transfers of personal data in connection with Medeaocean’s provision of the services. This includes the offshore access of EU/EEA personal data from third countries.
- **Countries of origin:** Mediaocean transfers personal data out of the EEA, UK, and Switzerland (together, "Europe") to both countries holding adequacy status under the European data protection law and countries without adequacy decisions, as outlined below.
- **Adequacy mechanism:** Where adequacy does not apply, Mediaocean relies on the EEA Standard Contractual Clauses (SCCs) as a transfer mechanism, see contractual measures below for more details.
- **Mediaocean’s Services**: Mediaocean’s services consist of SaaS-based advertising infrastructure, media planning, advertising data management, campaign orchestration and advertising delivery solutions. The scope of the data being transferred may depend on the solutions and supporting technical or professional services being provided.

EU Adequacy Decisions

Europe/EEA and Adequate Countries	• Bulgaria • Canada • France • Germany • Ireland • Israel • Japan • New Zealand • Netherlands • Poland • Sweden • United Kingdom • United States *(for businesses participating in the EU-US Data Privacy Framework and its Swiss and UK extensions)*	SCCs are enforceable.
Countries without Adequacy Decisions	• Australia • Costa Rica • India • Philippines • Serbia • Singapore • Taiwan	SCCs are enforceable.

Legitimacy of Transfers to the United States

The United States is Mediaocean's principal destination for data transfers from the European Union and Economic Area, or our other service locations where applicable.

- In **July 2020**, the Court of Justice of the European Union issued its long-awaited decision in Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems ("Schrems II"), holding that (1) the EU-US Privacy Shield program could no longer be used for data transfers to the United States, and (2) the transfer mechanisms identified in the GDPR—including the European Commission-issued Standard Contractual Clauses (SCCs)—could only be used where the laws and practices in the data importer's country do not impinge on the protections provided by the transfer mechanism.
- To address the concerns raised in the Schrems II decision, on October 7, 2022, President Biden signed **Executive Order 14086**, "Enhancing Safeguards for United States Signals Intelligence Activities", which implements changes to US foreign intelligence and redress practices in line with the EU - US Data Privacy Framework.
- On **10 July 2023** the European Commission adopted its adequacy decision for the EU-US Data Privacy Framework and Program, concluding it ensures US protection of personal data transferred between the countries is comparable to that offered in the EU/EEA.
- On **17 July 2023** the US Department of Commerce's International Trade Administration launched the Data Privacy Framework Program for businesses transferring EEA personal data to the US

- From **12 October 2023**, businesses in the UK can start to transfer personal data to US organizations certified to the "UK Extension to the EU-US Data Privacy Framework" (UK Extension) under Article 45 of the UK General Data Protection Regulation (GDPR) without the need for further safeguards such as those set out in Articles 46 and 49 of the UK GDPR.

The European Commission's adequacy analysis and the United Kingdom's companion analysis form the basis of this TIA.

Risk of Governmental Access Requests

Mediaocean believes there is little risk that the US government or other governments would collect the personal data we process about or on behalf of our business clients.

We do not believe ourselves to be an "Electronic Communications Service Provider" under Section 702 FISA with regard to the processing of personal data at issue and, thus, are likely out of probable scope of this and similar foreign intelligence laws. Further, we process a limited amount of business client relationship management, platform access and advertising transactional data which we believe is of little interest to national security and law enforcement interests.

That said, if we ever were to receive any kind of request from a governmental body requesting the personal data you have submitted to our Services, to the extent permitted by applicable laws, we would:

1. Attempt to fight or quash the request by raising nonfrivolous objections.
2. Provide affected clients with reasonable notice of the request so that you have the opportunity to seek a protective order or other appropriate remedy,
3. Attempt to redirect the governmental body to request the information from you directly.
4. If ultimately required to disclose your personal data to the government, limit the disclosure to the minimum amount of data legally necessary to comply with the request.

Technical and organizational measures

Mediaocean takes the privacy and security of client data seriously. To ensure that we meet state of the art practices for privacy and security, we have implemented the following technical, contractual, and organizational measures to protect the personal (and other) information within our care.

Technical measures

Mediaocean's technical safeguards are aligned to ISO 27001/2 standards and are implemented using security and data protection industry best practices. Our production systems are tested against the SOC 1 and SOC 2 Type II Trust Services Criteria.

- **Hosting locations:** Today Mediaocean leverages platform hosting locations in the US, EMEA, and APAC. While client data may leave a hosting region in some cases (for example, if a client employee opens a technical support request and one of our support engineers needs to access a client account to provide support), we ensure that client data is not stored in a separate region.
- **Encryption.** All client data is encrypted in transit using Transport Layer Security (TLS) with HTTP Strict Transport Security (HSTS) by default, and can be configured by our customers to use TLS 1.2 where supported. Moreover, all client data is encrypted at rest with FIPS 140-2-compliant encryption standards, as well as FIPS 140-2-approved cryptographic devices for the generation, storage, and revocation of encryption keys.

- **Data retention:** We rely on the principle of storage minimization to ensure that client data is not retained for longer than is necessary for your purposes. For more information on our default retention periods, please refer to our hosted systems privacy policies (US, EMEA, APAC).

If you require a copy of Mediaocean's latest SOC1 or SOC2 reports, please email datasecurity@mediaocean.com.

To learn more please visit our Information Security page.

Contractual measures

Mediaocean leverages Data Protection Agreements (DPA) with European Commission-approved Standard Contractual Clauses (SCC) to legitimize onward transfers of EEA and UK personal data. DPAs with SCCs are in place amongst Mediaocean group companies, with our vendors (Subprocessors) and with our clients.

Organizational measures

Mediaocean implements the following organizational measures to safeguard all client data transferred to us:

- **Vendor management.** Prior to onboarding a new Subprocessor, we conduct a comprehensive vendor assessment, which includes a review of the Subprocessor's security and privacy practices. Moreover, we require annual audit documentation from our Subprocessors to demonstrate compliance with the security terms of its data processing agreement.
- **Incident response planning**. We have a robust vulnerability management program in place to stay ahead of security incidents. We use many tools and tactics to discover security vulnerabilities, infrastructure scans, internal security testing, and annual third-party penetration tests. We also have a detailed incident response plan and dedicated incident response team that guides our investigation and mitigation of any identified or potential breach.
- **Business continuity planning.** We have a thorough business continuity plan designed so that our teams work diligently to recover operations in a timely manner, if needed.
- **Recurring audits.** We conduct annual SOC 1 and SOC 2 Type 2 audits to ensure compliance with our technical and organizational measures, and we make our relevant audit reports available to you.
- **Confidentiality obligations**. All of our employees are required to sign confidentiality agreements, where local law allows. In addition, all of our Subprocessors who handle client data are required to adhere to confidentiality terms.
- **Access controls.** We enforce strict access controls to ensure that the only people who have access to Customer Personal Data are those that absolutely need it to perform their job functions. To further ensure that this is the case, we log all access to Customer Data.
- **Employee training.** We provide privacy and security training to all of our employees when they join the company, and yearly thereafter. As a result, our employees are always kept up to date on security and privacy best practices.
- **Privacy by design.** To ensure that all of our Services are built with privacy in mind, we make sure that data protection reviews and considerations are explicitly included in the product design life cycle.

Transfer Impact Summary (all countries)

Purpose for transfer and any further processing	**Direct transfers:** Mediaocean employees may access personal data for the purposes of the provision of Services. **Onward transfers:** Mediaocean transfers client data to its Subrocessors for the purposes of assisting in the provision of Services
The frequency of the transfer	**Direct transfers:** Continuous. **Onward transfers:** Continuous.
Categories of personal data transferred	**Direct and onward transfers:** • User authentication details • Business contact information • Logs of actions taken by users within the platform • Support request details • Correspondence details
Categories of sensitive data transferred (if applicable)	**Direct and onward transfers:** • Determined by client
Subprocessors	**Onward transfers:** Please refer to Mediaocean's Subprocessor page
Applicable transfer mechanism	**Direct and onward transfers:** • Data Protection Agreement with EEA Standard Contractual Clauses
Contractual enforceability	• DPAs and SCCs are enforceable.