Chainalysis

Transfer Impact Assessment White Paper

March 27, 2023

Table of Contents:

About this white paper

This white paper provides customers of Chainalysis' web-based products (e.g., Reactor, KYT) with information to assist in conducting data transfer impact assessments of their use of such products. This document is intended specifically to facilitate customers' assessments in light of the (1) Schrems II ruling by the Court of Justice of the European Union (CJEU), and (2) recommendations[1] from the European Data Protection Board (EDPB) on supplementing safeguards under Article 46 of the GDPR with additional measures to ensure an EU-level of protection for personal data that is transferred to non-adequate jurisdictions.

In this white paper, we'll first provide some background on the Schrems II ruling and the EDPB recommendations. Then, we'll explain the measures taken by Chainalysis as a "data importer" under the Standard Contractual Clauses to provide an equivalent level of data protection for personal data that is transferred from the European Economic Area (EEA), Switzerland, and the United Kingdom (UK) in connection with our customers' use of our web-based products. Lastly, we'll provide an overview of our policies and practices that help protect customer data against inappropriate disclosure to law enforcement and other government agencies.

Unless otherwise noted, terms in this document have the meaning set forth in Appendix A.

Legal notice

This white paper is provided for informational purposes only and is not intended as legal advice. Customers and prospects are responsible for engaging their own legal counsel to advise on their specific situations and applicable compliance requirements, respectively, and are in the best position to do so.

Chainalysis' obligations to its customers are set forth in the parties' agreements, and this white paper does not modify or form a part of any such agreements. Nor does it create any commitments or assurances from Chainalysis or its affiliates, suppliers, or licensors.

The information here reflects Chainalysis' web-based offerings (e.g., Reactor, KYT) and related practices as of the time of its publication and not necessarily developments after such date. This page does not address Chainalysis' on-premise and professional service offerings, our training and certification programs, or our corporate IT systems.

[1] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, version 2.0, adopted on June 18, 2021, by the European Data Protection Board.

A. Background

1. The Schrems II decision

In its July 2020 Schrems II ruling[2], the CJEU invalidated the EU-U.S. Privacy Shield Framework as a valid mechanism for the transfer of personal data from the European Economic Area (EEA) to the United States. The CJEU, however, also held that the European Commission's Standard Contractual Clauses are a valid transfer mechanism for data transfers from the EEA to countries that do not have an "adequate" level of data protection under GDPR ("third countries"); provided, however, that data exporters also conduct due diligence to confirm that the personal data transferred is protected at a level equivalent to that under European data protection law, including putting in place any necessary "supplementary measures".

2. The EDPB Recommendations

After the Schrems II decision, the European Data Protection Board[3] issued the non-exhaustive, non-binding EDPB Recommendations to help data exporters assess transfers of personal data to third countries and determine what, if any, supplementary measures should be implemented to achieve the necessary level of data protection. The EDPB Recommendations outlined a six-step assessment ("EDPB Transfer Impact Assessment") as follows:

- Step 1: Perform a mapping of all data transfers to third countries and assess whether the data transferred is adequate, relevant, and limited to what is strictly necessary considering the purposes for which it is processed (i.e., "know your transfers").

- Step 2: Verify the transfer mechanism(s) on which each transfer relies (for example, a European Commission adequacy decision under GDPR Article 45, the Standard Contractual Clauses, a derogation under GDPR Article 49, etc.).

- Step 3: Assess whether the laws of the third countries and the practices of their government actors adversely impact the effectiveness of the transfer mechanisms. (The Standard Contractual Clauses also require the parties to assess the relevant transfer(s), the law and practices of the third country, and any relevant contractual, technical, or organizational safeguards to ensure that the data importer is not precluded from complying with the clauses.)

[2] Data Protection Commissioner v Facebook Ireland and Maximillian Schrems, Case C-311/18, Court of Justice of the European Union (CJEU), July 16, 2020.

[3] The European Data Protection Board (EDPB) is an independent body whose work focuses on the consistent application of the GDPR in the EU and cooperation between the EU's data protection authorities. The EDPB, which replaced the Article 29 Working Party in May 2018, consists of representatives of the national data protection authorities and the European Data Protection Supervisor (EDPS).

- Step 4: Identify and adopt any supplementary measures, such as contractual, technical, or organizational measures, that are otherwise necessary to bring the level of data protection in line with European standards.

- Step 5: Take any necessary procedural steps to adopt the supplementary measure(s).

- Step 6: At appropriate intervals, re-evaluate the level of protection afforded to the personal data that the data exporter transfers to third countries and keep abreast of any developments that could affect it.

B. Step 1: Know Your Transfer

This section helps customers perform Step 1 of the EDPB Transfer Impact Assessment, namely, determining whether the use of Chainalysis' web-based products results in a transfer of personal data to third countries and whether the data transferred is adequate, relevant, and limited to what is strictly necessary.

1. Location of application servers and database

Chainalysis' primary application servers and databases for its web-based products run on Amazon Web Services (AWS) data centers in the European Union[4], which are encrypted at rest using AES-256 or greater. The extent to which AWS servers store personal data will depend on the content that customers submit in their use of our products.

2. Data importer

When transferring personal data to Chainalysis outside of the European Economic Area, Switzerland, and the United Kingdom when using our web-based products, customers are the data exporters while Chainalysis Inc., the corporate group's parent company in the United States, is the data importer.

3. Third-party data processing

A list of Chainalysis sub-processors and additional information about them is available here, including instructions for how to subscribe to receive advance notifications regarding the engagement of new sub-processors. We may also transfer personal data about or from our customers to other categories of third parties as further explained in our Privacy Policy.

[4] Chainalysis uses data centers that are in a member state of the European Union. Chainalysis customers may contact their respective Customer Success Manager for additional information.

C. Step 2: Verify the transfer mechanism

This section helps customers perform Step 2 of the EDPB Transfer Impact Assessment, which is to verify the transfer mechanism on which it will rely to export personal data to Chainalysis.

When it is not possible for the parties to rely on (1) a valid finding of adequacy issued by the European Commission or UK Government (or other authority as applicable), (2) a mechanism, derogation, exemption, or exception that a customer is able to invoke (such as the data subjects' consent or a derogation under GDPR Article 49), or (3) a successor program to the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks, Chainalysis will rely on the Standard Contractual Clauses and/or the UK International Data Transfer Addendum. Both are incorporated by reference in Chainalysis' form of data processing agreement and remain valid data transfer mechanisms according to Schrems II, EDPB Recommendations, and regulatory guidance from the UK Information Commissioner's Office.

To be exact, Chainalysis will agree to both the Controller-to-Processor version of the Standard Contractual Clauses and the Controller-to-Controller version of the Standard Contractual Clauses. The Controller-to-Processor clauses apply to transfers of customer data to a third country when Chainalysis is a processor, and the Controller-to-Controller clauses apply to transfers of customer data to a third country where Chainalysisis a controller. The Chainalysis intercompany data transfer agreement also incorporates the Standard Contractual Clauses.

D. Step 3: Assess the laws of the third country and the transfer tools you are relying on

This section helps customers perform step 3 of the EDPB Transfer Impact Assessment, which is to assess the risk of inappropriate disclosure of personal data from Chainalysis, as the data importer, to law enforcement and intelligence agencies. The information presented below is based on the laws and practices of the recipient country, in this case, the United States, and the EDPB's Recommendations 02/2020 on the European Essential Guarantees for surveillance measures[5].

1. Data transfers to the United States

The Schrems II ruling primarily focuses on law enforcement's authority in the United States to engage in the surveillance of individuals, particularly for national security purposes. Below, we address the specific U.S. laws that were discussed in the ruling and their relevance to the use of Chainalysis products:

[5] Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, adopted on November 10, 2020, by the European Data Protection Board. Guarantee A: Processing should be based on clear, precise and accessible rules. Guarantee B: Necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated. Guarantee C: An independent oversight mechanism should exist. Effective remedies need to be available to the individual.

- Foreign Intelligence Surveillance Act (FISA), Section 702 ("FISA § 702") – Permits U.S. government authorities to conduct surveillance targeting and compel disclosure of information about non-U.S. persons who are located outside the U.S. to gather foreign intelligence information.
- Executive Order 12333 ("EO 12333") - Authorizes intelligence agencies (like the U.S. National Security Agency (NSA)) to conduct surveillance outside of the U.S. It provides authority for U.S. intelligence agencies to collect foreign "signals intelligence" information from communications and other data that is accessible by radio, wire, and other electromagnetic means (e.g., underwater cables).

(a) Foreign Intelligence Surveillance Act (FISA)

FISA § 702 permits U.S. government authorities to conduct surveillance targeting and compel disclosure of information about non-U.S. persons who are located outside the U.S. for the purposes of gathering foreign intelligence information. The source of the information sought, however, must be a U.S.-based "electronic communication service provider" or a "remote computing service provider" under the Electronic Communications Privacy Act (ECPA), and the order must be approved by the Foreign Intelligence Surveillance Court in Washington, DC.[6]

In particular, FISA § 702 authorizes "upstream" collection (UPSTREAM) and "downstream" collection (formerly, PRISM) of data. As the name implies, upstream collection refers to the indirect upstream collection of communications via telecommunications providers that provide the "backbone" of the Internet, for example, Verizon and AT&T. Upstream data collection, which the CJEU noted as problematic in the Schrems II ruling, has been described as a form of "backdoor" surveillance by the government because downstream providers will generally not have any knowledge of the data collection. According to highly-confidential U.S. government records leaked by Edward Snowden in 2013, U.S. governmental agencies and their surveillance programs appeared to be focused on a limited number of large U.S. "Internet backbone" and telecommunications service providers, whose businesses are materially different from that of Chainalysis.

Downstream collection, on the other hand, authorizes U.S. authorities to target and collect data directly from U.S.-based electronic communications service providers. To the extent Chainalysis receives such a request for customer data, we will review the request as per the policies set forth below in Section E(2) on "Government access to data".

In 2018, the United States enacted additional safeguards to FISA § 702 via amendments that included: (i) annual government submission and FISC approval of querying, targeting, and minimization procedures; (ii) improvements of the Privacy and Civil Liberties Oversight Board's[7] ability

[6] For more information on FISA § 702, see the Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, June 2, 2014 by the Privacy and Civil Liberties Oversight Board.

[7] The Privacy and Civil Liberties Oversight Board is an independent agency within the Executive Branch established by the 9/11 Commission Act of 2007. "The Board's mission is to ensure that the federal government's efforts to prevent terrorism are balanced with the need to protect privacy and civil liberties."

to conduct oversight; (iii) requirements to maintain privacy and civil liberties officers by the NSA and FBI; (iv) expanded whistleblower protections to contract employees at intelligence agencies; and (v) additional transparency requirements on the government, including to disclose the number of FISA § 702 targets annually.

In response to the Schrems II ruling, the U.S. Department of Commerce[8] confirmed that important limits and safeguards exist regarding the U.S. government's ability to access data pursuant to FISA § 702:

- Access to company data for national security purposes, as highlighted by Schrems II, are "unlikely to arise because the data they handle is of no interest to the U.S. intelligence community." Companies handling "ordinary commercial information like employee, customer, or sales records, would have no basis to believe U.S. intelligence agencies would seek to collect that data."
- There is an individual redress for violations of FISA § 702 that is available to EU citizens but was not addressed by the court in the Schrems II ruling. These include provisions that allow private claimants to seek compensatory and punitive damages.

(b) Executive Order 12333, United States Intelligence Activities

EO 12333 makes different U.S. intelligence agencies responsible for certain overt and clandestine intelligence and counterintelligence activities and also places restrictions on those activities. EO 12333 does not, unlike FISA § 702, authorize the U.S. government to require companies to disclose data let alone "in bulk". Despite the concerns of the CJEU in Schrems II, U.S. law does not allow the government to require companies in the United States to disclose data for intelligence purposes without statutory authorization and the targeting of specific persons or identifiers, e.g., FISA § 702. Accordingly, Chainalysis cannot be ordered to take any action to facilitate the type of bulk surveillance under EO 12333 that was raised in the Schrems II ruling.

Bulk data collection by the government is permitted in other scenarios, however, such as clandestine intelligence activities involving overseas access to data. Indeed, the Schrems II court was concerned about the U.S. government's ability under EO 12333 to intercept personal data in transit to the U.S. via telecommunications infrastructure, e.g., transatlantic cables. Notwithstanding the fact that companies cannot be legally compelled to participate in such activities, and many governments, including the United States and EU Member States, collect intelligence information outside of their territories[9], personal data can be protected from such interception using technical measures such as encryption. Please see Section E(1) below on "Technical measures" for more information about how Chainalysis uses encryption measures to address these risks.

(c) Clarifying Lawful Overseas Use of Data Act (CLOUD Act)

---

[8] U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II, September 2020, prepared by the U.S. Department of Commerce in conjunction with the Department of Justice and the Office of the Director of National Intelligence.
[9] U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II, September 2020.

The CLOUD Act amended the Electronic Communications Privacy Act (ECPA), which is a U.S. law that prescribes how law enforcement agencies may obtain information from certain technology companies, including cloud service providers. Notably, the CLOUD Act creates a new framework governing cross-border law enforcement requests, including limitations on U.S. law enforcement's ability to request data. For example,

- The CLOUD Act does not permit bulk surveillance. The CLOUD Act only permits the U.S. government to access data in criminal investigations after obtaining a warrant based on probable cause of a specific crime from an independent court.
- When the digital content in question is owned by an enterprise, the U.S. Department of Justice has stated it will "seek data directly from the enterprise, rather than its cloud-storage provider, if doing so will not compromise the investigation."
- The CLOUD Act also explicitly allows companies to challenge disclosure requests in court and make conflicts of law arguments.[10]

2. Data transfers to other countries

Chainalysis is not aware of any applicable laws or regulations in other countries besides the United States that prevent Chainalysis from fulfilling our contractual obligations on the processing of personal data, or posing any materially different privacy risks of inappropriate disclosure of personal data to government law enforcement and intelligence agencies. Conversely, and as explained by the U.S. Department of Commerce, the "theoretical possibility that a U.S. intelligence agency could unilaterally access data being transferred from the EU without [Chainalysis'] knowledge is no different than the theoretical possibility that other governments' intelligence agencies, including those of EU Member States, or a private entity acting illicitly, might access the data."[11]

E. Steps 4 and 5: Identify and adopt supplementary measures

This section helps customers with Steps 4 and 5 of the EDPB Transfer Impact Assessment by summarizing supplementary measures that support an equivalent level of protection for personal data exported from the EU by customers to Chainalysis. The EDPB Recommendations provide a non-exhaustive list of supplementary measures, which fall into the following three categories:

- Technical measures, such as encryption and logging;
- Contractual measures, including commitments with respect to law enforcement requests for data; and
- Organizational measures, for instance, internal policies and processes, and adoption of codes of conduct.

[10] What is the CLOUD Act? by BSA | The Software Alliance (outlining the scope of the CLOUD Act).

[11] U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II, September 2020.

Below is a list of technical, contractual, and organizational supplementary measures Chainalysis that has implemented to safeguard personal data transferred by our customers to Chainalysis in the United States, in line with the EDPB Recommendations and our obligations under the Standard Contractual Clauses (as the data importer).

1. Technical measures

As part of our value of building trust, Chainalysis provides a robust security and privacy program, including technical measures to protect personal data against unauthorized access. We have a security management program and review our Information Security Management Program (ISMP) annually. Chainalysis is SOC 2 certified, which attests to our compliance with Security and Confidentiality. An overview of Chainalysis' privacy and security controls is available in our Privacy and Security White Paper, which can be provided upon request.

Notably, a key technical measure described in the EDPB Recommendations is encryption. Chainalysis' products rely on industry-standard encryption services to protect communications during transmissions between a customer's network and the products. Traffic between the client and the Chainalysis products is encrypted through TLS with secure algorithms enabled. Encryption between Chainalysis customers and Chainalysis applications is enabled using a minimum HTTPS TLS 1.2 authenticated tunnel. Connections to the Chainalysis network and databases are obtained through a secured IPSEC tunnel, only accessible from within the production network. Clients' sessions and interactions are encrypted using 256-bit SSL V3/TLS HTTPS. Customer data in Chainalysis is further secured by an SDLC process that implements security best practices and controls for its applications such as AES 256-bit encryption for data at rest, monitoring and logging, vulnerability management, and system hardening.

2. Contractual measures

(a) Data processing agreements

Chainalysis signs data processing agreements with customers containing the mandatory GDPR Article 28 provisions, including commitments to take certain measures to protect customers' personal data. For example, Chainalysis agrees to (i) implement appropriate technical and organizational measures to protect personal data that it processes in its capacity as a processor, and (ii) may provide third-party audit reports, if any, upon request so that customers can verify compliance.

(b) Standard Contractual Clauses

In particular, Chainalysis signs data processing agreements with its customers that incorporate the Standard Contractual Clauses. The Standard Contractual Clauses contain a number of protections with respect to international data transfers and compelled disclosure of data by government actors. After the Schrems II ruling, the 2021 version of the clauses was promulgated by the European Commission and approved by all EU Member States to provide some mechanism for a lawful transfer of personal data from the EEA to third countries. The EDPB Recommendations explicitly noted that the Standard Contractual Clauses can help address the issue of government entities' access to personal data that was raised in the Schrems II decision. Chainalysis has also incorporated the Standard Contractual Clauses in its intercompany data transfer agreement, which covers transfers

between Chainalysis affiliates. See the section below on “Government access to data” for more information on our policies for handling compelled disclosure requests from government entities.

3. Organizational measures

We’ve put a number of organizational safeguards in place to protect personal data and support our adherence to the contractual commitments noted above.

(a) Government access to data

Chainalysis treats the information a customer submits to our web-based products as “confidential information” under its customer contracts. We do not, as a result, share such information with government actors as a matter of course.

In the event of a compelled disclosure request, Chainalysis has internal processes for individually reviewing and responding to requests from government entities to access data in compliance with our contractual commitments and legal obligations. Chainalysis will abide by the following in the event a government entity seeks access to confidential customer data:

- Chainalysis will not make disclosures without appropriate legal process, such as a validly issued subpoena, court order, or search warrant.
- We review all government requests for information to ensure they are valid and not overbroad before responding. We will reject requests which are legally insufficient.
- We will provide our customers with prior notice in the event we receive a legally-binding request, unless we are prohibited from doing so by law.
- Where appropriate, Chainalysis may seek to narrow the scope of requests or ask that the requesting government entity liaise directly with the customer.
- Chainalysis will provide data as specified in the legal order and only to the extent necessary as reasonably determined by Chainalysis in its sole discretion.

Like all companies, however, Chainalysis may be required to respond to lawful demands from government entities to provide customer data or information for specific customer accounts, for instance, pursuant to a validly issued search warrant or court order.

(b) Information security policies

Chainalysis’ security policies, standards, and procedures are updated and approved annually by relevant stakeholders such as the Information Security and Privacy teams as well as at the executive level. Please see the Chainalysis Privacy and Security White Paper for additional information on our organizational measures.

(c) Third-party management

We require service providers to undergo a thorough cross-functional review process by subject matter experts in our Security, Privacy, and Risk & Compliance Teams to ensure our customers’ personal data receives adequate protection. This process includes reviewing the data to be shared with the service provider, the provider’s security policies, controls, and third-party audits, how the

provider addresses data transfer restrictions along with any supplementary measures, whether the supplier has a sufficiently mature privacy program, and the resulting risks.

We also provide a list of our sub-processors available here, including instructions for how to subscribe to receive advance notifications regarding the engagement of new sub-processors.

(d) Privacy and security training

Chainalysis makes internal privacy and security policies and data protection training available to all employees.

F. Step 6: Re-evaluate the level of data protection at appropriate intervals

As per Step 6 of the EDPB Recommendations, Chainalysis will assess the then-current transfer tools and supplementary safeguards for sufficiency at appropriate intervals in light of any developments to the applicable data privacy laws and frameworks.

As an example, Chainalysis will closely follow the EU-U.S. Data Privacy Framework, which was announced by President Biden and European Commission President von der Leyen in March 2022. This framework will replace the EU-U.S. Privacy Shield that the CJEU invalidated in Schrems II, and may provide an important mechanism for transatlantic transfers of personal data from the European Union to the United States.

Specifically, President Biden signed an Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities. This order outlines steps that the United States will take to implement its commitments under the proposed EU-U.S. Data Privacy Framework[12], including safeguards that limit access to data collected via U.S. surveillance activities to validated intelligence priorities in a proportional manner, requires intelligence agencies to update their policies and procedures accordingly, establishes an independent and impartial redress mechanism, and enhances oversight of surveillance intelligence gathering. Chainalysis will consider participation in the framework if and when the framework is formally granted adequacy by the European Commission.

[12] Fact Sheet: President Biden Signs Executive Order to Implement the European Union-U.S. Data Privacy Framework, October 7, 2022.

Appendix A

DEFINITIONS

Controller	means the entity which, alone or jointly with others, determines the purposes and means of the processing of personal data.
Data Subject	means the identified or identifiable person to whom personal data relates.
Standard Contractual Clauses	Standard Contractual Clauses for the transfer of personal data to third countries as approved by the European Commission's Implementing Decision (EU) 2021/914 of 4 June 2021.
GDPR	means Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.
Personal Data	means any information relating to an identified or identifiable natural person.
Processing or Process	means any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Processor	means the entity which processes personal data on behalf of the controller.
Sub-Processor	means any agent, subcontractor, or other third party (excluding its employees) engaged by Chainalysis or a Chainalysis affiliate for carrying out any processing activities of personal data on behalf of the controller.
UK International Data Transfer Addendum	International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, version B1.0, in force March 21, 2022, as issued by the United Kingdom Information Commissioner's Office under Section 119A(1) of the Data Protection Act of 2018.

Appendix B

Chainalysis Affiliates

Entity Name	Country
Chainalysis Inc.	United States
Chainalysis Canada Inc.	Canada
Chainalysis Government Solutions, LLC	United States
Chainalysis ApS	Denmark
Chainalysis B.V.	Netherlands
Chainalysis UK Ltd	United Kingdom
Chainalysis Pty Ltd	Australia
Chainalysis Japan Co., Ltd.	Japan
Chainalysis Pte. Ltd.	Singapore
Chainalysis Korea Ltd.	South Korea