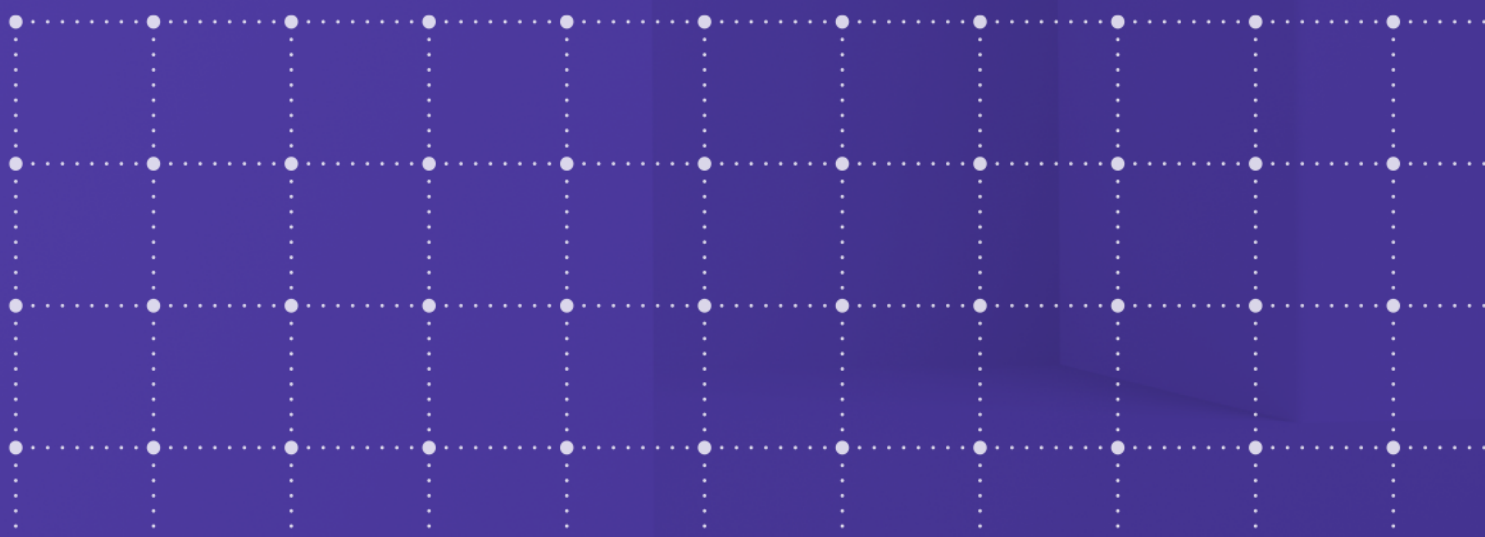
Abnormal

Transfer Impact Assessment (TIA) and Transfer Risk Assessment (TRA)

Version 1.0

Updated Jan 30, 2023

This document provides information about the privacy and security of Abnormal Security Corporation's ("Abnormal") software-as-a-service platform ("Service") which can help our customers to assess the Abnormal security and privacy program. It does not provide legal advice. We urge you to consult with your own legal counsel to familiarize yourself with the requirements that govern your specific situation.



Overview

Abnormal recognizes that our customers, because of their obligations as data controller(s) under the General Data Protection Regulation ("GDPR") (or similar privacy frameworks), will take steps to perform privacy impact assessments when considering our cybersecurity products. While we are not able to provide legal advice nor perform a privacy impact assessment on behalf of any of our customers, Abnormal understands our obligation as a data processor under GDPR (or similar privacy frameworks) to reasonably assist our customers in their compliance efforts, including in the completion of privacy impact assessments.

This document provides information about the privacy and security of the Abnormal Service which can help our customers assess the Abnormal security and privacy program. In particular, this document describes the legal regimes applicable to Abnormal in the United States, the safeguards Abnormal puts in place in connection with transfers of customer personal data from the European Economic Area or countries with similarly privacy frameworks, and Abnormal's ability to comply with its obligations as a data processor under the Standard Contractual Clauses ("SCCs").

Answers to the most common questions about data transfers and contractual, organizational and technical measures regarding the Abnormal Service may be found in the 'Abnormal Security Data Impact Assessment FAQ' made available at security.abnormalsecurity.com.

Background

On July 16, 2020, in *Schrems II*, the Court of Justice of the European Union (CJEU) invalidated the EU-U.S. Privacy Shield framework (Privacy Shield), holding that the Privacy Shield was no longer a valid legal mechanism for ensuring that personal data transferred to third countries located outside of the European Union (EU) met minimum safeguards to protect the rights and freedoms of EU citizen data subjects. In the same case, the CJEU upheld the use of Standard Contractual Clauses (SCCs) – also commonly known as "Model Clauses" – as a valid tool to cover transfers of personal data outside the EU. Thus, parties conducting transfers of personal data from the EU to the United States (US) and certain other third countries, should assess the adequacy of the SCCs on a case-by-case basis, and supplement the SCCs with additional measures where appropriate.

In *Schrems II*, the CJEU also raised concerns regarding the US government's mass surveillance programs conducted under FISA 702 (a US law setting up a judicial review process to follow for authorizing the US government's collection of a specific type of foreign intelligence data) and EO 12.333 (a US Executive Order that is the organizing source of US intelligence gathering programs).

After the *Schrems II* decision, the European Data Protection Board ("EDPB") issued non-legally binding guidance for data exporters performing transfer impact assessments in its Recommendations 01/2020 on measures to supplement transfer tools to ensure compliance with the EU level of protection of personal data ("EDPB recommendations"). The EDPB recommendations provides a non-exhaustive list of protections companies can take when transferring personal data from Europe to Third Countries to ensure an essentially equivalent level of protection for the data that is transferred.

The EDPB Recommendations outlined the following six-step approach for conducting transfer impact assessment (EDPB Transfer Impact Assessment):

- **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.
- **Step 2: Identify Data Transfer Mechanism(s)**. Verify the transfer tool(s) on which the transfer relies.
- **Step 3: Assess the Laws or Practices of the Third Countries**. These laws or practices may impinge on the effectiveness of the appropriate safeguards of the transfer tool, including using Recommendations 02/2020 on the European Essential Guarantees for surveillance measures.
- **Step 4: Adopt Supplementary Measures**. If the laws or practices of the Third Countries mean 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 European standard of essential equivalence.
- **Step 5: Adopt Necessary Procedural Steps**. Take any formal procedural steps the adoption of any 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.

On December 13, 2022, the European Commission launched a process towards the adoption of an adequacy decision for the EU-US Data Privacy Framework, which will foster safe trans-Atlantic data flows and address the concerns raised by the Court of Justice of the European Union in its Schrems II decision. The draft decision concludes that the US legal framework, based on Executive Orders signed by President Biden on October 7, 2022, provides comparable safeguards to those of the EU and ensures an adequate level of protection for personal data transferred from the EU to US companies. Once the adequacy decision is adopted, then European entities will be able to transfer personal data to participating companies in the United States, without having to put in place additional data protection safeguards.

Until the adequacy decision is adopted by the European Commission, Abnormal uses the EDPB Transfer Impact Assessment to demonstrate that the risks involved in transferring and processing European personal data in/to the US does not impinge on our ability to comply with our obligations under the SCCs or to ensure that individuals' rights remain protected. Even if an adequacy decision is adopted by the European Commission (or in the absence of an adequacy decision), Abnormal intends to continue to use the EDPB Transfer Impact Assessment and the SCCs to ensure that individuals' rights remain protected under applicable privacy frameworks.

Step 1: Identify International Data Transfers

Where Abnormal processes personal data governed by European data protection laws (or similar privacy frameworks) as a data processor, Abnormal complies with its obligations under the Abnormal Security Data Processing Addendum ("DPA").

The Abnormal DPA incorporate the SCCs and provide the following information:

- Description of Abnormal's processing of customer personal data (Annex I);
- Description of Abnormal's security measures (Annex II); and
- UK GDPR SCCs Addendum for making Restrict Transfers (Exhibit 2)

Abnormal has implemented appropriate safeguards to ensure that customer personal data remains protected whenever it is processed by our sub-processors, including entering into data processing agreements and transfer mechanisms (such as the SCCs) and implementing supplementary measures where necessary. Abnormal also has a process in place to review the privacy and security controls for sub-processers that have access to customer personal data. A list of all of our data sub-processors is available on our Trust Center and our 'Abnormal Security Sub-Processor TIA & TRA' is available at security.abnormalsecurity.com.

For the purposes of providing you the Service, Abnormal may transfer customer personal data in the United States. For a detailed FAQ about the type of personal data processed by the Service, please see our Product Privacy Guide.

Step 2: Identify Data Transfer Mechanisms

Where personal data originating from Europe (or countries with similar privacy frameworks) is transferred to Abnormal, Abnormal relies upon the European Commission's SCCs to provide an appropriate safeguard for the transfer. To review the Abnormal DPA (which incorporates the 2021 SCCs) please visit this page.

Where customer personal data originating from Europe (or countries with similar privacy frameworks) is transferred between Abnormal to third-party sub-processors, Abnormal enters into data protection agreements and SCCs with those parties.

Step 3: Assess the Laws or Practices of the Third Countries

The *Schrems II* ruling focused European attention on the breadth of law enforcement powers, particularly with respect to national security requirements that permits US government agencies to engage in proactive surveillance. To address these issues, we have set out specific information about certain US laws considered by the CJEU ruling and their application to Abnormal in this Section

Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II Whitepaper

In response to *Schrems II* ruling, the Department of Commerce issued a whitepaper outlining the limits and safeguards in the US relating to government access to data, notably that:

- Most US companies do not deal in data that is of any interest to US intelligence agencies and therefore do not pose a risk of the nature highlighted in Schrems II;
- Companies whose EU-US transfers of personal data involving ordinary commercial information would have no basis to believe US intelligence agencies would seek to collect that data;
- 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;
- 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.

U.S. Surveillance Laws

FISA 702 and Executive Order 12333

The following US laws were identified by the Court of Justice in the European Union in *Schrems II* as being potential obstacles to ensuring essentially equivalent protection for personal data in the United States:

- FISA Section 702 ("FISA 702") - allows US government authorities to compel disclosure of information about non-US persons located outside the US for the purposes of foreign intelligence information gathering. This information gathering must be approved by the Foreign Intelligence Surveillance Court in Washington, D.C. In-scope providers subject to FISA 702 are electronic communication service providers within the meaning of 50 U.S.C. §1881(b)(4), which can include remote computing service providers ("RCSP"), as defined under 18 U.S.C. §2510 and 18 U.S.C. §2711.
- Executive Order 12333 ("EO 12333") - authorizes intelligence agencies (like the US National Security Agency) to conduct surveillance outside of the United States. In particular, it provides authority for US intelligence agencies to collect foreign "signals intelligence" information, being information collected from communications and other data passed or accessible by radio, wire and other electromagnetic means. This may include accessing underwater capables carrying internet data in transit to the United States. EO 12333 does not rely on the compelled assistance of service providers, but instead appears to rely on exploiting vulnerabilities in telecommunications infrastructure.

US Clarifying Lawful Overseas Use of Data Act ("Cloud Act")

The CLOUD Act, enacted in 2018, clarifies existing legal frameworks and retains meaningful limitations on US law enforcement's ability to request data. The CLOUD Act further confirms that the physical location of data is not the deciding factor but whether the recipient of a request has "possession, custody, or control" of the data. Requests are subject to the existing high standards and procedures for making such a request. The CLOUD Act also established additional safeguards, including explicitly allowing companies to challenge disclosure requests that conflict with another country's laws. For more information on the CLOUD Act, review What is the CLOUD Act? by BSA Software Alliance outlining the scope of the CLOUD Act.

The whitepaper notes:

- 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

Is Abnormal subject to FISA 702 or EO 12333?

Abnormal, like most US-based SaaS companies, could technically be subject to FISA 702 where it is deemed to be a RCSP. However, Abnormal does not process personal data that is likely to be of interest to US intelligence agencies.

Furthermore, Abnormal is not likely to be subject to upstream surveillance orders under FISA 702, the type of order principally addressed in, and deemed problematic by, the Schrems II decision. Abnormal does not provide internet backbone services, but instead only carries traffic involving its own customers. The Abnormal Service processes and stores a limited subset of a customer's data necessary to enable the Service to perform its email security function. Most customer data is stored within the customer's own email tenant or the tenant of the customer's cloud storage environment. To date, the U.S. Government has interpreted and applied FISA 702 upstream orders to only target market providers that have traffic flowing through their internet backbone and that carry traffic for third parties (i.e., telecommunications carriers).

EO 12333 contains no authorization to compel private companies (such as Abnormal) to disclose personal data to US authorities and FISA 702 requires an independent court to authorize a specific type of foreign intelligence data acquisition which is generally unrelated to commercial information. In the event that US intelligence agencies were interested in the type of data that Abnormal processes, safeguards such as the necessity and proportionality requirements would protect data from excessive surveillance.

What is Abnormal's practical experience dealing with government access requests?

The EDPB Recommendations say that data exporters should take into account the data importer's practical experience "with relevant prior instances of requests for access received from public authorities" outside Europe. To date, Abnormal has never received a US National Security Request (including access under FISA 702 or direct access under EO 12333 in connection with customer personal data). Therefore, while Abnormal may technically be subject to the surveillance laws identified in Schrems II, we have not been subject to these types of requests in our day-to-day business operations.

Our Process

If Abnormal ever receives a request for user information from a government agency or law enforcement agency from any jurisdiction, Abnormal will notify its customers, unless legally prohibited. Additionally, our legal team will review the request to ensure there is a valid legal basis for the request.

Requests Received

The report below includes information about any such requests that Abnormal has received, except as prohibited by applicable law. This report is updated annually.

Requests Received for User Information from Government Agencies or Law Enforcement Official from Any Jurisdiction

Reporting Period	Number of Requests Received	Number of Impacted Users
2018	0	0
2019	0	0
2020	0	0
2021	0	0
2022	0	0

**This report is aggregated and anonymized, and does not identify any particular individual, company, or request.*

Step 4: Adopt Supplementary Measures

Abnormal provides the following **technical measures** to secure data:

- **Encryption**: Abnormal offers data encryption at rest and in transit.
- **Security**: Abnormal maintains an internal Information Security Program (ISP) that addresses our products and our general business practices. The ISP ensures a secure environment for our personnel, customers, systems, and the data we are entrusted to handle. Our ISP is designed to implement appropriate technical and organizational measures covering our product environment and related company systems, cover key areas such as access controls; personnel training; physical security; network and cloud security; credential and key management; and software development life cycle policies and practices.
- **SOC 2 certification**: Our ISP is audited on at least an annual basis by a third-party auditor in connection with a SOC 2 audit. We maintain a SOC 2 certification as a result of this regular audit activity and can share the most recent SOC 2 report with our customers on request and under a non-disclosure agreement. The SOC 2 is a report based on the Auditing Standards Board of the American Institute of Certified Public Accountants' (AICPA) existing Trust Services Criteria (TSC). The purpose of this report is to evaluate an organization's information systems relevant to security, availability, processing integrity, confidentiality, and privacy.
- **ISO 27001 certification**: Coalfire ISO, Inc. certifies that Abnormal operates an Information Security Management System (ISMS) that conforms to the requirements of ISO/IEC 270i01:2013.
- More information about Abnormal's security practices and certifications is made available at https://security.abnormalsecurity.com/.

Abnormal's **contractual measures** are set out in our Legal Center and Data Processing Addendum, which incorporates the SCCs. In particular, we are subject to the following requirements:

- **Technical measures**: Abnormal is contractually obligated to have in place appropriate technical and organisational measures to safeguard personal data (both under our DPA as well as the SCCs we enter into with customers and service providers).
- **Transparency**: Abnormal is obligated under the SCCs to notify its customers in the event it is made subject to a request for government access to customer personal data from a government authority. In the event that Abnormal is legally prohibited from making such a disclosure, Abnormal is contractually obligated to challenge such prohibition and seek a waiver.
- **Actions to challenge access**: Under the SCCs, Abnormal is obligated to review the legality of government authority access requests and challenge such requests where they are considered to be unlawful.

Abnormal's **organizational measures** to secure data include:

- **Policy for government access**: With respect to government and law enforcement requests or demands for information or data, including requests made under FISA 702, Abnormal's policy is to refrain from sharing or disclosing any data in response to such a request or demand unless and until the validity of the order or demand can be confirmed. Abnormal will carefully review such requests or demands, engaging counsel where appropriate, and will take legal steps to notify customer(s) or other parties who may be impacted by or are the subject of the request prior to complying with the request. In addition, Abnormal will seek to narrow the scope of such a request or demand where it is overbroad, or otherwise resist where its basis or validity are in question.
- **Onward transfers**: Whenever we share your data with third-party service providers, we remain accountable to you for how it is used. We require all service providers to undergo a thorough cross-functional diligence 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 a review of the data Abnormal plans to share with the service provider and the associated level of risk, the supplier's security policies, measures, and third party audits, and whether the supplier has a mature privacy program that respects the rights of data subjects. A list of our sub-processors is made available at security.abnormalsecurity.com/ and our 'Abnormal Security Sub-Processor TIA & TRA' is available at security.abnormalsecurity.com.
- **Employee training**: Abnormal provides data protection training to all Abnormal staff.

Step 5: Adopt Necessary Procedural Steps

When assessing potential data protection risks in relation to compelled disclosures and international data transfers post-Schrems II, the GDPR requires that data importers and data exporters take into account the specific circumstances of the transfer and any safeguards put in place (including relevant contractual, technical, and organizational measures applying to Personal Data). In other words, a holistic approach is required in which the entire array of contractual, technical, and organizational security measures offered by Abnormal and those that can be implemented by customers needs to be considered so that an appropriate risk assessment can be made. The GDPR does not require that organizations eliminate all risk, which would be impossible, but to take appropriate measures to mitigate risks.

In light of the information provided in this document, including the technical, contractual, and organizational measures Abnormal has implemented to protect customers' personal data, Abnormal considers that the risks involved in transferring and processing European personal data in/to the US does not impinge on Abnormal's ability to comply with its 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

Abnormal 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.