International Data Transfers with Sentry

Overview

Sentry is committed to enabling our customers to use Sentry's services in compliance with data protection regulations, including the General Data Protection Regulation ("**GDPR**").

This document is intended to provide information about international transfers of European personal data that we process on our customers behalf in connection with Sentry's services. Sentry has self-certified to the EU-U.S. Data Privacy Framework, the UK Extension to the EU-U.S. Data Privacy Framework, and the Swiss-U.S. Data Privacy Framework (collectively, the "**DPF**") with respect to the processing of European personal data. We transfer European personal data to the United States under the DPF Principles but also offer the European Commission's Standard Contractual Clauses as an alternative mechanism to transfer personal data from Europe in compliance with the GDPR.

While a transfer impact assessment is not required under the DPF, we've prepared this document to help our customers conduct their own due diligence in connection with use of Sentry's services. In doing so, we've considered the European Data Protection Board recommendations on international data transfers ("**EDPB Recommendations**", available here).

This document is split into six parts, reflecting the assessment steps outlined in the EDPB Recommendations, and includes a description of the legal regimes applicable to Sentry in the United States and the measures taken by Sentry to protect customer data.

Part 1: Know your transfer

What is the nature of Sentry's services?

Sentry offers a suite of software-as-a-service solutions designed to identify, monitor and alert its customers to problems that are occurring in their application, website or other service. Additional information about our company and our services is available here and here.

What is the nature of the data being transferred?

We offer our services to customers around the world, which means we may process personal data relating to individuals in the European Economic Area, United Kingdom and Switzerland ("**Europe**"). With respect to such processing, we comply with our obligations under our Data Processing Addendum.

Please refer to Schedule 1 of our Data Processing Addendum for further information about the personal data we process on our customers' behalf, including the type of personal data we process and the categories of data subjects. Note our Data Processing Addendum includes an express prohibition on the transfer of special categories of personal data to Sentry.

Where does Sentry process personal data?

Sentry is headquartered in the United States and we also have group companies in Canada, Austria, the Netherlands, and other countries. We currently host our product infrastructure in the United States and Germany. We also use other sub-processors to help provide our services, including our cloud infrastructure providers, as described below.

Does Sentry onward transfer the data to any third parties?

Yes. We share customer personal data with certain of our group companies and other third-party sub-processors. Please see our current list of sub-processors here.

Part 2: Identify transfer tool relied on

Mechanisms to enable the transfer of personal data in compliance with the GDPR are incorporated into our Data Processing Addendum and form part of our customer agreements — please refer to Schedule 3 of our Data Processing Addendum.

Data Privacy Framework: Sentry has self-certified to the EU-U.S. Data Privacy Framework, the UK Extension to the EU-U.S. Data Privacy Framework, and the Swiss-U.S. Data Privacy Framework (collectively, the "**DPF**"), as set forth by the U.S. Department of Commerce, with respect to the processing of personal data received from Europe. Sentry processes European personal data in compliance with the DPF Principles. To view our DPF certification, please see here.

The DPF has been granted adequacy by the European Commission and UK authorities for transfers of personal data to the United States. Per current guidance, Sentry relies on the DPF to receive personal data from the EEA and UK in the United States. Sentry intends to rely on the DPF for equivalent transfers of personal data from Switzerland once the Swiss Federal Administration's officially recognizes the adequacy of the Swiss-U.S. DPF.

Standard Contractual Clauses: Where Sentry is transferring personal data to a jurisdiction not benefitting from an adequacy decision, Sentry relies on the European Commission's Standard Contractual Clauses ("**SCCs**") as an alternative mechanism. The SCCs are a legally valid transfer mechanism and form part of our customer agreements – please refer to Schedule 3 of our Data Processing Addendum.

Where we transfer personal data originating from Europe between Sentry group companies or to our other third-party sub-processors, Sentry also enters into SCCs with those parties.

Part 3: Assess whether the transfer tool relied upon is effective in light of the circumstances of the transfer

Is Sentry aware of any surveillance laws in the United States that enable government authorities to access personal data?

Yes, Sentry is aware of certain laws in the United States that enable government agencies to access personal data for surveillance, intelligence and criminal law enforcement purposes. In particular, the Court of Justice of the European Union concluded in "*Schrems II*" that Section 702 of the Foreign Intelligence Surveillance Act ("**S702 FISA**") and Executive Order 12333 ("**EO 12333**") authorize US government surveillance programs in a manner that may interfere with the protection of personal data transferred to the United States.

- S702 FISA is a federal law that allows US government agencies to conduct targeted surveillance of foreign persons located outside the United States with the compelled assistance of electronic communications service providers ("**ECSPs**") within the meaning of 50 U.S.C § 1881(b)(4). This includes "electronic communication service providers" and "remote computing service providers" as defined under 18 U.S.C. § 2510 and 18 U.S.C. § 2711, telecommunications carriers as defined under 47 U.S.C. §153, other communication service providers that have access to wire or electronic communications, and other relevant entities that are officers, employees or agents of the foregoing.

- EO 12333 authorizes and governs the circumstances in which US intelligence agencies can engage in foreign intelligence surveillance outside the United States. It authorizes collection of the content of communications of foreign communications that occur outside the United States in the course of a lawful foreign intelligence investigation. Unlike S702 FISA, EO 12333 does not rely on the compelled assistance of electronic communications service providers but appears to rely on exploiting vulnerabilities in telecommunications infrastructure.

In October 2022, President Biden issued EO 14086 to introduce new safeguards for U.S. signals intelligence activities. EO 14086 was designed to address the concerns raised by the Schrems II ruling and serves as the basis of the DPF adequacy decision. Firstly, the law places new requirements on the collection and handling of personal data by U.S. intelligence agencies, requiring that signals intelligence activities be "necessary" and "proportionate" and expanding the oversight of signals intelligence activities and subjects bulk data collection to tighter controls. Secondly, it creates a new redress mechanism for European individuals who claim their personal data was collected unlawfully through U.S. signals intelligence programs, including the opportunity for review by the Data Protection Review Court within the Department of Justice.

The European Data Protection Board has confirmed that the safeguards enacted through EO 14086 are not limited to transfers made through the DPF and therefore data exporters should take into account the safeguards under EO 14086 when assessing the effectiveness of both the DPF and other mechanisms (e.g., the SCCs) for transfers to the United States.

Is Sentry subject to S702 FISA or EO 12333?

Like most US-based cloud computing providers, Sentry may technically qualify as an "electronic communications service provider" within the scope of S702 FISA and therefore US government authorities could (at least theoretically) compel access to personal data that we process.

However, customers should note that Sentry does not generally deal in the type of data that is of interest to US intelligence agencies. As detailed in the US Department of Commerce's white paper titled "*Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II*" (available online at https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF), companies whose European operations involve data transfers limited to commercial information (such as employee, customer or sales records) are not the target of US intelligence and counter-terrorism agencies.

At the same time, EO 12333 does not contain an authorization to compel private companies (such as Sentry) to disclose personal data to US authorities.

The information that Sentry processes as part of our business is primarily commercial information. Where US agencies are interested in the type of data that Sentry processes, safeguards such as the requirement for authorization by an independent court and the necessity and proportionality requirements should protect data from excessive US surveillance.

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

Sentry publishes a Transparency Report semi-annually to provide our customers with greater visibility about data requests by governmental entities and law enforcement.

Customers should note that, to date, Sentry has never received any government agency requests for access to personal data from Europe under US surveillance laws. We are also not aware of any direct access to personal data originating from Europe under EO 12333. Therefore, while Sentry may technically be subject to US surveillance laws, we do not receive these types of requests in our day-to-day business operations.

Part 4: Identify the technical, contractual and organizational measures to protect the data

What safeguards has Sentry implemented to protect personal data?

We have implemented a number of technical, organizational and contractual measures to protect personal data that we process on behalf of our customers.

We provide the following technical measures to protect personal data:

- **Encryption**. All data sent to Sentry is encrypted at rest and in transit. Additional details on Sentry encryption practices are available in Schedule 2 of our Data Processing Addendum.

- **Other Security Practices**. Additional details on Sentry's other security practices, including with respect to access control, application security, infrastructure and network security, and business continuity and disaster recovery is set forth Schedule 2 of our Data Processing Addendum.

- **Certifications**. Sentry's suite of solutions is SOC2 and/or ISO 27001 certified. Our third-party certifications and audit reports are available to customers in-product or upon request.

We provide contractual measures as set out in our Data Processing Addendum to protect personal data. This includes the following:

- **Security Commitments**. Sentry is required to have in place appropriate technical and organizational measures to safeguard personal data and to ensure sub-processors also contractually commit to implement and maintain equivalent security measures to protect personal data.

- **Transparency.** Sentry is required to notify our customers of any requests for access to customer's personal data from a government authority, unless prohibited to do so by law. In the event of such legal prohibition, Sentry is obligated to seek a waiver of such prohibition. Further, Sentry is required to generally notify our customers if we can no longer comply with the SCCs, without being required to identify the specific provision with which we can no longer comply.

- **Non-Cooperation with Access Requests.** Sentry is required to never comply with any request under S702 FISA for bulk surveillance, i.e., a surveillance demand whereby a targeted account identifier is not identified via a specific "targeted selector" (an identifier that is unique to the targeted endpoint of communications subject to the surveillance). Sentry is also required not to take any action pursuant to EO 12333.

- **Actions to Challenge Access.** Sentry is required to use all available legal mechanisms to challenge any demands for data access through national security process that Sentry receives.

We provide the following organizational measures to protect personal data:

- **Onward Transfers**. Sentry has implemented rigorous due diligence checks by our Security and Legal & Compliance teams to ensure that our sub-processors can provide sufficient guarantees to implement appropriate technical and organizational measures to keep personal data secure. As a part of this due diligence process, where required, Sentry conducts a transfer risk assessment for each sub-processor and the surveillance laws of the sub-processor's country. Where necessary, Sentry implements supplementary measures with our sub-processors to further protect data from interception by government authorities.

- **Employee Training**. All Sentry employees receive data privacy training.

Part 5: Procedural steps necessary to implement effective supplementary measures

In light of the above information, including Sentry's practical experience dealing with government requests and the technical, contractual and organizational measures we have implemented to protect personal data, Sentry considers that the risks involved in transferring personal data from Europe to the United States and other countries in connection with our services do not impinge on our ability to comply with the SCCs or ensure that individuals' rights remain protected. Therefore, no additional supplementary measures are necessary at this time.

Part 6: Re-evaluate at appropriate intervals

Sentry will review and, if necessary, reconsider the risks involved and the measures it has implemented to address changing data privacy regulations and enforcement activity associated with transfers of personal data outside Europe.

Last updated: January 19, 2024

This document is for information purposes only and reflects our current product offerings and practices (which are subject to change without notice). Customers are responsible for making their own independent assessment of the information contained in this document. This document does not form part of or modify any agreement customers may have with Sentry, nor does it create any commitments or assurances from Sentry or our group companies or sub-processors.