CORELIGHT DATA TRANSFER IMPACT ASSESSMENT GUIDE

Last Updated: November 1, 2025

This document provides information in connection with customers' use of Corelight products and services ("**Corelight Offerings**") to assist in conducting a transfer impact assessment of customer personal data from the European Economic Area ("**EEA**"), United Kingdom or Switzerland ("**Europe**") in light of recommendations from the European Data Protection Board ("**EDPB**"). It also describes the supplementary measures that Corelight offers to protect customer personal data.

Overview

Transfers to Corelight

Corelight Offerings are made available globally, and in limited circumstances, may involve transfers of personal data. Under certain global privacy laws, including those of Europe, personal data cannot be transferred outside of the EEA unless: (i) the importing country has been deemed by the respective privacy authorities to have an adequate level of protection, or (ii) the data exporter has appropriate safeguards in place to ensure that the personal data transferred is subject to an adequate level of protection.

Where Corelight processes personal data governed by European data protection laws on behalf of our customers (as a data processor), Corelight complies with its obligations under Corelight's customer Data Processing Addendum ("**DPA**").

Corelight's customer DPA: (i) incorporates the Standard Contractual Clauses (SCCs) and (ii) provides a description of Corelight's processing of customer personal data (Schedule 1) along with a description of the applicable Corelight Offering's security measures.

Subprocessor Transfers

Corelight's provision of the Corelight Offerings does involve the transfer of customer personal data to subprocessors. The subprocessors relevant to a particular customer will depend on one or more of the following: data center region, the Corelight Offering purchased, and the product-specific features that a customer enables and/or opts to use. A list of Corelight's Subprocessors (including their purpose and location) as well as a mechanism for subscribing to subprocessor updates is available here.

Transfer Tool

When transferring customer personal data to a jurisdiction not benefitting from an adequacy decision, Corelight currently relies on the implementation of the SCCs and supplementary measures for international data transfers. The Court of Justice of the European Union recognized the SCCs as a legally valid transfer mechanism subject to a case-by-case basis analysis of the transfer. Exporting controllers and processors must conduct transfer impact assessments for transfers to the U.S. or to any third country when relying upon the SCCs. The most recent set of SCCs are those pursuant to Regulation 2016/679 and were released in 2021; these SCCs are incorporated into Corelight's DPA available here.

When customer personal data originating from Europe is transferred by Corelight to third-party subprocessors, Corelight ensures that a legally valid transfer mechanism is in place (typically the SCCs accompanied by supplementary measures as applicable).

Effectiveness of Transfer Tool

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

To date, Corelight has not received any government requests for access to customer data (including any personal data contained therein) and is not aware of any governmental unauthorized access, and Corelight has not provided such data to governments. Corelight has not provided backdoors to any government. Corelight also has procedures in place for responding to law enforcement requests in the event that Corelight receives such a request.

Does Corelight publish a transparency report?

To date, Corelight has never received a request from a government authority to access customer personal data and therefore has not published a transparency report. Should those circumstances change, Corelight will re-evaluate publishing transparency reports at such time.

Is Corelight subject to the surveillance laws identified in Schrems II?

While Corelight may generally be subject to the U.S. surveillance laws identified in Schrems II, Corelight's day-to-day operations have not been impacted by government access requests and the types of customer personal data processed by Corelight on behalf customers are not likely to be of interest to U.S. intelligence agencies.

- *FISA 702*: As defined in Sections 2510 and 2711 of Title 18 U.S.C., respectively, Corelight may act as electronic communications services ("ECS") and also potentially as remote computing services ("RCS") in connection with the Corelight Offerings we provide to customers. Corelight is therefore among the large number of U.S. companies upon which the U.S. government could technically serve a targeted directive under FISA 702. However, as the U.S. government has applied FISA 702, Corelight is not eligible to receive the type of order that was of principal concern to the CJEU in the Schrems II decision—i.e., a FISA 702 order for "upstream" surveillance. As the U.S. government has applied FISA 702, it uses upstream orders solely to target traffic flowing through internet backbone providers that carry Internet traffic for third parties (i.e., Google, Yahoo). Corelight does not provide such Internet backbone services. As a result, it is unlikely that Corelight would receive the type of order principally addressed in the Schrems II decision.
- *EO 12333*: EO 12333 is a general directive organizing U.S. intelligence activities and does not include any authorization to compel private companies to disclose data.

As noted above, Corelight has never received a request from a government authority to access customer personal data.

Supplementary Measures

In addition to the SCCs, Corelight offers a number of supplementary measures to ensure that customer personal data remains protected when it is transferred outside Europe. These measures include:

Contractual Measures

Corelight contractually commits to appropriate data protection and privacy measures under our DPA. Corelight regularly reviews and updates our DPA to reflect applicable data privacy requirements, including:

- *SCCs*: Corelight's customer DPA incorporates the SCCs to transfer customer personal data to countries outside Europe.
- *Processing in accordance with instructions*: Corelight commits to processing customer personal data in accordance with the customer's instructions.

- ***Subprocessors***: Corelight is transparent about the use of subprocessors, making its list of Corelight Subprocessors available <here>. Corelight enters into written agreements with Subprocessors that include data protection and security measures consistent with the measures Corelight offers to its customers.

Technical Measures

Corelight designs our offerings to help customers protect their data and comply with global regulations.

- ***Hosting Options***: Corelight's cloud product allows customers to select the location in which their data is hosted.
- ***Security Measures***: the specific security measures applicable to certain offerings are described here.
- ***Audits***: Corelight performs annual audits of its cloud product's security measures according to SOC 2 standards, as detailed in Corelight's Trust & Compliance self-service portal.

Organizational Measures

Corelight has implemented company-wide policies and procedures:

- ***Security and privacy programs***: Corelight maintains comprehensive information security and data privacy programs that include appropriate measures designed to protect customer data.
- ***Employee training***: Corelight requires all employees to complete information security and data protection and privacy training upon hire and then once a year at a minimum.
- ***Vendor Management***: Corelight screens and vets third-party vendors.

Additional Information

To help customers further perform a transfer impact assessment and understand how customers can address their data protection requirements, Corelight encourages customers to review the DPA, Trust Center and applicable security measures, as well as Documentation for details specific to the Corelight Offering. If customers have any questions regarding these documents, please contact privacy@corelight.com.