Corelight Investigator

Data Privacy FAQs

Last Updated: April 8, 2026

Corelight understands the significance of customer data and that customer data may be subject to various global privacy laws and regulations. This document outlines Corelight's approach to privacy with respect to Corelight Investigator, including its AI Features.

Corelight's "**AI Trust FAQs**" (available at www.corelight/com/trust-center) describe in more specificity how the capabilities of Corelight's AI Features work.

Can customers use Corelight Investigator in compliance with the GDPR?

Corelight Investigator – including its AI Features – supports compliance with the GDPR and other global data protection and privacy laws:

- Corelight Investigator has implemented the technical and organizational security measures (detailed here) to protect customer data.
- Corelight's DPA includes key GDPR-related assurances and incorporates the Standard Contractual Clauses ("**SCCs**") approved by the European Commission to address transfers of personal data outside of the EU, Switzerland, and the UK.
- Corelight supports hosting options globally and customers have the ability to select their Corelight Investigator deployment region.

Is customer data transferred to subprocessors?

Yes, Corelight uses certain infrastructure and other third-party subprocessors to provide Corelight Investigator – including its AI Features – to customers. The subprocessors applicable to a specific customer's deployment depend on the hosting region selected along with the services and functionalities used by that customer. A list of Corelight's subprocessors is available at www.corelight.com/legal/subprocessors.

When Corelight transfers data globally, it does so in compliance with applicable law, including entering into data processing agreements and approved transfer mechanisms (such as the SCCs) where appropriate.

- With respect to Corelight Investigator's AI Features, Corelight leverages a third-party hosted LLM. Corelight Investigator's AI Features use OpenAI's GPT series of models, accessed via API. When Corelight Investigator's optional AI Features are enabled, customer data is processed for one-time inference only and is not stored or used for training purposes. For more details, please see Corelight's ZDR approach described in the section regarding supplementary measures below.

What appropriate safeguards does Corelight rely on to transfer customer personal data outside of the EU?

Corelight is a global company and we may transfer customer personal data originating from the EEA, Switzerland, or the UK to Corelight's non-European locations, as well as to those third-party subprocessors that are necessary to provide our offerings. In such cases, Corelight relies on the SCCs and appropriate addenda for transfers of personal data outside of the EU, Switzerland, or the United Kingdom.

What measures does Corelight implement to protect customer personal data that is transferred outside of the EU?

- Corelight Investigator implements the technical and organizational security measures specified in our Security Measures, which forms a part of the DPA, to safeguard and protect the confidentiality and security of the customer personal data that is transferred.
- With respect to Corelight Investigator's AI Features, Corelight has established a Zero Data Retention (ZDR) agreement with OpenAI, its LLM provider.
    - OpenAI's ZDR policy means customer data is not stored or used for training.
    - ZDR enables data security by contractually guaranteeing that OpenAI uses customer data only for processing the immediate task and does not store it.
    - Corelight's ZDR approach helps customers comply with regulations like the GDPR.

Does Corelight maintain a transfer impact assessment for its offerings?

Please see Corelight's Data Transfer Impact Assessment Guide.