FAQs

Collibra, customer data and data privacy

Collibra recognizes that our customers entrust us with the care of their data. Given the importance of data to our customers, we aim to be as transparent as possible as to what customer data we process and how it is treated. This document addresses frequently asked questions about Collibra's processing of customer data, including personal data, on behalf of our customers, and our compliance with data privacy requirements with respect to such data.

This document does not cover Collibra's processing of contact information provided by customers for customer account administration purposes, nor does it cover information Collibra collects from individuals via its websites or in connection with marketing/industry events and activities. These forms of processing are governed by our Privacy Policy.

What customer data does Collibra process?

There are two categories of customer data which Collibra processes within the Collibra Platform, **Platform Data** and **Source Data:**

- **Platform Data** is the data that is stored in the Collibra Platform as a primary storage location. It consists of metadata describing customers' underlying Source Data (see below), enterprise data governance structures and other forms of non-sensitive data. Platform Data can include personal data, such as contact information and roles and titles of users of the Collibra Platform, user account access credentials, information about users' use of the Collibra Platform (i.e. usage analytics), and IP addresses. Platform Data represents the majority of customer data processed within the Collibra Platform.
- **Source Data** is the data comprising our customers' own data sets, or samples or subsets of such data, originating from separate, customer-controlled data sources (e.g. AWS, GCP, Snowflake, Databricks, etc.), which may be submitted by customers to the Collibra Platform for analysis or temporary viewing. Source Data can represent any form of data, including personal data. Collibra minimizes the processing of Source Data to the extent possible, including through technical protocols such as our Edge functionality. In addition, the only Source Data processed by Collibra is the Source Data which customers expressly submit to the Collibra Platform for analysis or temporary viewing.

What does Collibra do with the customer data?

Collibra processes both Platform Data and Source Data as necessary to provide its services. We also analyze Platform Data (but not Source Data) for our own, internal product improvement and analytics purposes, including analyzing Collibra Platform usage behavior (pseudonymized) and content (aggregated across customers) reports. This analysis helps us continue to improve the quality of products and services we provide as well as enhance our customers' experience in leveraging them. Collibra processes this customer personal data in accordance with our Data Processing Addendum.

Does Collibra share customer personal data with third parties?

In order to provide our services to customers, Collibra shares personal data of customers with the subprocessors identified here. Our subprocessor list is updated from time to time as we add new vendors. As described in our Data Processing Addendum, Collibra notifies its customers via email 30 days in advance of providing new subprocessors customer data.

In what regions is Collibra's customer personal data processed, and how does it ensure international data transfers are conducted in a privacy compliant manner?

Access to and other processing of customer personal data may occur from or within countries where Collibra and its subprocessors operate or host data, as applicable. A list of Collibra's business locations as well as the location from or within which our subprocessors access or process our customers' data is provided here. With respect to the hosting of a customer environment, a customer may designate an available hosting region on its Collibra order form.

In the event customer personal data subject to protections under the GDPR or the UK GDPR is transferred outside of the EU or UK, it is conducted pursuant to Collibra's adherence to the EU-U.S. Data Privacy Framework or the UK Extension thereto, or where such frameworks are not applicable, the EU GDPR Standard Contractual Clauses and/or the UK GDPR Standard Contractual Clauses. A copy of Collibra's Transfer Impact Assessment on the transfer of EU or UK customer personal data to the U.S., Australia and India is available to customers and prospective customers upon request.

Collibra was recently approved for Binding Corporate Rules for Processors (BCRs) by the Belgian Data Protection Authority, which will support international transfers of personal data going forward. These BCRs will operate in conjunction with Collibra's continued adherence to the EU-US Data Privacy Framework as well as EU/UK GDPR Standard Contractual Clauses.

How does Collibra vet its subprocessors?

Collibra conducts robust data privacy and security diligence on all of its subprocessors of customer personal data and holds its subprocessors to the same data privacy and security standards as customers hold Collibra pursuant to binding, written agreements, including data processing addenda.

What privacy regulations does Collibra comply with?

Collibra focuses its privacy compliance on the regimes to which the data of the majority of our customers is subject. The majority of our customers demand GDPR and CCPA compliance, and therefore Collibra complies with both. We review our compliance with additional regulatory regimes on a case-by-case basis.

How long does Collibra store customer data?

Data from customer environments is available for customers to export for a period of 30 days after expiration or termination of their agreements with Collibra. Customer environments are subsequently deleted between 90 and 120 days after termination or expiration of a contract.

What security protocols does Collibra maintain within customer environments?

Please see our Security Policy.

What additional safeguards does Collibra have in place with respect to the transfer of EU or UK personal data to the U.S. and other non-EU countries?

In addition to being certified to the EU-U.S. Data Privacy Framework and UK Extension thereto, Collibra has taken the following steps when transferring customer personal data outside of the EU and UK:

- Within its current Data Processing Addendum, Collibra has incorporated the most recent version of the EU Standard Contractual Clauses, and solely to the extent applicable, the UK Addendum to the EU Standard Contractual Clauses
- A Transfer Impact Assessment addressing our customers' transfer of European data subjects' personal data to the U.S., India and Australia to avail themselves of Collibra's services is available to customers and prospective customers upon request
- Collibra was approved for Binding Corporate Rules for Processors (BCRs) by the Belgian Data Protection Authority in December 2023

How does Collibra handle U.S. government requests or inquiries for customer personal data?

Collibra has never received requests to disclose customer personal data from U.S. authorities, whether under Section 702 of the U.S. Foreign Intelligence Surveillance Act (FISA) Amendments Act of 2008, U.S. Executive Order 12333 of Dec. 4, 1981 or otherwise. Given the history of these requests and the nature of the data Collibra processes, Collibra does not expect to receive such requests in the future. Nevertheless, if Collibra were to receive such a request, it would immediately inform the relevant customer data exporter, as permitted by U.S. law. In certain circumstances, however, government authorities are allowed to request an order prohibiting the disclosure of such requests from a U.S. court. If such an order were granted, Collibra would be required to abide by its terms. Please note that with respect to redress mechanisms, Collibra does certify to the EU-U.S. Data Privacy Framework and UK Extension thereto.

