

Avallone Data Retention

How Avallone works with retention and deletion of data

Introduction and data categorization

Avallone is an AML/KYC tool. Therefore, we see data retention and GDPR regulation as a core responsibility to solve for our users. This document outlines how Avallone works with data retention and deletion.

In terms of data categorization, it is important to note that Avallone does not process sensitive data as defined in the EU GDPR regulation. (That is: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs; trade-union membership; genetic data, biometric data processed solely to identify a human being; health-related data; data concerning a person's sex life or sexual orientation.)

However, Avallone understands the confidential and critical nature of the data that is stored and processed on the platform and has several safeguards to protect the data as described in our security documents.

Retention policies

There is a significant difference between companies' internal retention policies - due to the differences between local regulations and adoptions of EU law. Therefore, Avallone believes that the individual customer should decide when data should be permanently deleted. Any deletion process in the Avallone platform always starts with a user's actions, hence, nothing is deleted automatically without a user initiating the process.

The various situations where deletion would be initiated are:

- Replacing information: e.g. when changing the name of a legal entity - the current information will be deleted and replaced with the new information
- Removing data: when removing a group of data - e.g. all data related to an individual or a legal entity - the data will be moved to the "archived folder," where it stays until final deletion
- Deleting documents: when deleting a document, the document will be moved to the "archived folder," where it stays until final deletion

Data which is stored in an archived folder will, by default, be deleted after five years. If a customer requires a specific storage time (i.e. shorter or longer than five years), then this can be agreed upon with Avallone, and we will adjust the storage period for the various archived data types.

On-demand, our customers can pull a report with an overview of all archived data with specified deletion dates. On request, data can be deleted before the defined deletion date.

Module specific retention policies

Avalone Hub

Legal entities

- When removing a legal entity from the company list, the entire legal entity will be moved to the “Archived” list.
- When a legal entity is archived, all data related to “details”, “documents”, “Q&A”, and “activities” will be deleted after five years.
- All relations to legal entities and officers will be deleted right away. The same goes for officers' roles in the legal entity.

Officers

- When removing an individual from the officer list, the individual will be moved to the “archived” list.
- When an individual is archived all data related to “details”, “documents”, “relations”, and “activities” will be deleted after five years.
- All the information will be stored in a pdf report that can be downloaded together with documents (if any).

Documents

- For both individuals and legal entities, documents can be archived individually by clicking on “Delete document”.
- When the document is deleted it is moved to the “archived” list, the documents will be available in the archived list and deleted after five years.

Information

- When information is replaced (e.g. a name, address or a TIN number), the current information will be deleted and replaced with the new information.
- It is also possible to replace information with an empty field.
- It is not possible to restore replaced information.

KYC Responder

Responder cases

- It is possible to delete a responder case that is in draft mode.
- If a case is deleted, all information and documents are deleted, and it would not be possible to restore them.
- Responder cases that have been handled and marked as done will be moved to the “done” list. Closed cases will be deleted after five years.

Documents

- It is possible to delete uploaded documents in a specific responder case.
- When a document is deleted, it will not be possible to restore it.

Information

- When information (e.g. a name, address, or a TIN number) is replaced in one of the questionnaires, the current information will be deleted and replaced with the new information.
- It is also possible to remove information from a questionnaire.
- It is not possible to restore removed and replaced information.

KYC Collector

Counterparties

- It is possible to delete a counterparty that has not been a part of a request.
- When deleting the counterparty, it will not be possible to restore the information.
- On-demand, customers can ask Avallone to delete relevant counterparties from the platform.

Collector cases

- Data and questionnaires from a collector case are stored on each of the counterparty's profiles.
- Therefore, the information from a collector case will be deleted when a counterparty is deleted.
- The actual collector case will be stored as documentation for the process on the “closed” list.