

v1.4 (14.07.2025)

# fiskaly SAFE Service

This page describes the fiskaly SAFE service, whose purpose is to store fiscal data defined by law via API and fiskaly HUB, while following the required conditions - reliability, security, persistence and supported file formats.

## 1. Product Options

- 1.1. fiskaly offers the SAFE service in two product options “SAFE” and “SAFE flex”.

## 2. Product Description

### 2.1. Related to product option SAFE

- 2.1.1. SAFE is directly integrated into fiskaly HUB UI, where SIGN and/or DSFinVK Customers can activate or deactivate the archiving service based on the selected group. All connected SIGN and/or DSFinVK services will be automatically archived, based on the frequency the Customer sets at the fiskaly HUB.
- 2.1.2. SAFE supports the compliant archival of electronic accounting records that must be retained under applicable tax and commercial laws, including but not limited to digitally stored bookkeeping data, invoices, and audit trails.
- 2.1.3. By choosing a specific group, SAFE exports data from the customers related SIGN and/or DSFinVK services and archives the export files in the SAFE service. The archiving process itself follows the principles for the proper management and retention of books, records and documents in electronic form and for data access: unalterability, order, completeness and traceability.
- 2.1.4. The customer can search and retrieve data directly from the fiskaly HUB or via SAFE API.

### 2.2. Related to product option SAFE flex

- 2.2.1. SAFE flex provides an API that supports the compliant archival of electronic accounting records that must be retained under applicable tax and commercial laws, including but not limited to digitally stored bookkeeping data, invoices, and audit trails.
  - 2.2.2. The form, scope and content of the documents subject to recording and retention (data, data records and documents in electronic or paper form) are determined by the taxpayer. The archiving process itself follows the principles for the proper management and retention of books, records and documents in electronic form and for data access: unalterability, order, completeness and traceability.
- 2.3. Proof of audit-proof archiving can be provided for the duration of the statutory retention periods up to 10 years after the end of the year in which the respective data is sent in.
  - 2.4. The Customer is solely responsible for checking the individual retention period.
  - 2.5. fiskaly will provide unalterability for the individual retention period beginning after complete receipt of the data.
  - 2.6. fiskaly does not carry out any examination of data records in terms of content, legal or tax issues.
  - 2.7. The data is archived in certified Google Cloud data centres in Germany.

- 2.8. The fiskaly SAFE service supports the customer in exporting the archived data in accordance with the applicable legal requirements for the type and form of data export in connection with auditing by the tax authorities.

### 3. Functionalities

#### 3.1. Related to product option SAFE

- 3.1.1. The fiskaly HUB enables the transfer of data from fiskaly SIGN and/or DSFinVK solutions to the archive, specifically:

- SIGN DE
  - Archiving of TSS export (tar) files,
  - Export of the archived TSS files,
- DSFinVK
  - Archiving of DSFinV-K files,
  - Export of archived DSFinV-K export (tar) files,
- SIGN AT
  - Archiving of DEP7 files,
  - Export of archived DEP7 files,
- SIGN ES:
  - Archiving of XML files,
  - Export of archived XML files,
- SIGN IT:
  - Archiving of XML files,
  - Export of archived XML files,
- SIGN FR:
  - Archiving of XML files,
  - Export of archived XML files,

#### 3.1.2. Compliant Data Archiving via API and fiskaly HUB

SAFE provides a UI at the fiskaly HUB, which allows the archival of fiscal data in compliance with legal standards. The fiskaly HUB allows data transfer from SIGN and/or DSFinVK services to the archive.

##### 3.1.2.1. Archiving of DSFinV- files

SAFE supports DSFinV-K export files from fiskaly DSFinVK.API service to the archive. fiskaly does not validate the content and structure of the archived files.

##### 3.1.2.2. Archiving of TSS export files

SAFE supports TSS export files from fiskaly SIGN DE API. fiskaly does not validate the content and structure of the imported file.

##### 3.1.2.3. Archiving of DEP7- files

SAFE supports DEP7 export files from fiskaly SIGN AT.API service to the archive. fiskaly does not validate the content and structure of the archived files.

##### 3.1.2.4. Archiving of DEP131 export files

SAFE supports DEP131 export files from fiskaly SIGN AT API. fiskaly does not validate the content and structure of the imported file.

**3.1.2.5. Archiving of XML export files**

SAFE supports XML export files from fiskaly SIGN ES API. fiskaly does not validate the content and structure of the imported file.

**3.1.2.6. Archiving of XML export files**

SAFE supports XML export files from fiskaly SIGN IT API. fiskaly does not validate the content and structure of the imported file.

**3.1.2.7. Archiving of XML export files**

SAFE supports XML export files from fiskaly SIGN FR API. fiskaly does not validate the content and structure of the imported file.

**3.1.3. No validation of files and data records/ responsibility of the customer**

fiskaly does not perform any validation regarding the content, structure, compliance, completeness, or correctness of any imported files or datasets. Likewise, the provider does not review or verify the annotations, metadata, or field selections made by the customer. Responsibility for regulatory compliance and accuracy of the submitted data lies solely with the customer.

**3.1.4. Search and Export of Archived Fiscal Data**

The customer can search and export selected data for analysis, reporting, or regulatory submissions. Thanks to the standardized file format, seamless further processing in country-specific tools is possible.

**3.1.4.1. Search and export of archived DSFinV-K data**

DSFinV-K data can be searched by multiple criteria based on the defined annotations upfront, gather the list of files to be exported and trigger the export.

- created\_at (created date of Document- DSFinV-K ZIP File),
- retention\_period\_days (duration of storage of the document in accordance with legal requirements),
- start\_date (start date of the exported data),
- end\_date (end date of the exported data, may coincide with the start date),
- client\_id (optional: List of Client IDs)

The exported ZIP file contains all DSFinV-K data based on the selected criteria. ZIP file has multiple folders. Each DSFinV-K export zip file contains the files legally specified in the DSFinV-K documentation.

**3.1.5. Search and export of archived TSS data**

TSS data can be searched by multiple criteria based on the defined annotations upfront, gather the list of files to be exported and trigger the export.

- created\_at (document creation date),
- retention\_period\_days (retention period of the document in accordance with legal requirements),
- start\_date (start date of the exported data),
- end\_date (end date of exported data, may coincide with start date),

- tse\_id (ID of the TSS),
- client\_ids (optional: List of Client IDs).

The exported TAR file contains all TSS log files based on the selected criteria. The TAR archive file contains all log files defined by the TR (Technische Richtlinie).

### **3.1.6. Search and export of archived DEP7 data**

DEP7 data can be searched by multiple criteria based on the defined annotations upfront, gather the list of files to be exported and trigger the export. The exported file contains all log files based on the selected criteria.

### **3.1.7. Search and export of archived XML data**

XML data can be searched by multiple criteria based on the defined annotations upfront, gather the list of files to be exported and trigger the export. The exported file contains all log files based on the selected criteria.

## **3.2. Related to product option SAFE flex**

3.2.1. The API enables the integration of point-of-sale (POS) systems and supports the secure and compliant transfer of data to an archival system. Specifically, the API provides:

- An upload interface for export data files from certified technical security devices (e.g. cryptographically secured transaction logs),
- An upload interface for structured POS transaction data in a standardized format defined by applicable national legal or regulatory frameworks,
- Export functionality for both types of imported/uploaded data sets,
- Upload and export functionality for procedural documentation (main documentation and supplementary records), supporting the formats XML, JSON, CSV, PDF, ZIP, and HTML.

### **3.2.2. Compliant Data Archiving via API**

SAFE flex provides an API that supports the archival of fiscal data in compliance with legal standards. The API allows integration from POS systems, allowing for data transfer to the archive.

### **3.2.3. Upload of Supported Fiscal Export Sources**

SAFE flex supports export files generated by fiscal systems and APIs, including those based on applicable national specifications in Austria, Spain, Italy, Croatia, Liechtenstein, Slovakia, Switzerland, Slovenia, Hungary, France, and other jurisdictions. These may include fiscal data exports mandated by local authorities, as well as structured transaction reports produced by certified or registered systems ("Fiscal Data"). Fiscal Data includes structured data sets whose syntax is specified by law or by the tax authorities, for example, ("Standardized Fiscal Data").

### **3.2.4. Upload of Additional Documents in Supported Formats**

SAFE flex further supports the processing of procedural and legally relevant documents in commonly used technical formats such as XML, JSON, CSV, PDF, ZIP, and HTML. These formats are accepted for import and archival, provided they meet the general syntactic requirements of the underlying data transmission mechanisms.

### **3.2.5. No validation of files and data records/ responsibility of the customer**

fiskaly does not perform any validation regarding the content, structure, compliance, completeness, or correctness of any imported files or datasets. Likewise, the provider does not review or verify the annotations, metadata, or field selections made by the customer. Responsibility for regulatory compliance and accuracy of the submitted data lies solely with the customer.

### **3.2.6. Search Through Archived Fiscal Data**

The customers can locate specific files within archived data, allowing access for audits, refund validation, and internal reviews based on the defined annotations upfront. This ensures data is both accessible and retrievable to meet legal or business needs.

### **3.2.7. Search of the imported Standardized Fiscal Data**

Standardized Fiscal Data can be searched by multiple criteria based on the defined annotations upfront.

### **3.2.8. Search for all other applicable documents**

All other applicable documents can be searched based on the defined annotations upfront.

### **3.2.9. Export of Archived Fiscal Data**

The customer can export selected data for analysis, reporting, or regulatory submissions, with exports formatted for compatibility with standard systems.

### **3.2.10. Export of the imported Standardized Fiscal Data files**

Structured data files can be searched one or using multiple criteria based on the predefined annotations, and then the list of files to be exported can be compiled and the export can be triggered. The exported ZIP file contains all Standardized Fiscal Data data based on the selected criteria. ZIP file has multiple folders. Each Standardized Fiscal Data export zip file contains the files legally specified in the applicable Standardized Fiscal Data documentation.

### **3.2.11. Export of all other applicable documents**

All other applicable documents can be searched based on the defined annotations upfront. The exported files contain all other applicable document files based on the selected criteria.

## **3.3. Revision secure archive and audit logs**

3.3.1. All user actions - file uploads, access, views, and exports - are logged, providing full transparency and auditability. Each log is assigned a cryptographic hash to verify its integrity. Audit logs for each organization can be exported, allowing auditors to verify the historical integrity of archived files.

3.3.2. SAFE utilizes an audit mechanism that writes an audit log for every operation in the system. There is an independent audit trail for each organizational unit. The audit logs are chained together using a cryptographic hash.

- 
- OwnedBy: Organizational unit for which the file was archived
  - LogNumber: Monotonically increasing, unique number
  - Operation: Unique name of the operation (e.g.: file-archived)
  - Timestamp: Timestamp generated by the application(unqualified)
  - PreviousHash: Hash value of the previous log
  - CurrentHash: Hash value of the current log
  - HashAlgorithm: The hash function used (e.g.: SHA-256)
  - AuditEvent: Operation-dependent data (e.g. file size for file upload)
  - UserIdentifier: Unique identification of a user in the fiscal context

3.4. The customer can individually define the storage period for the artifacts mentioned. Deletion or modification of data, regardless of whether it is stored artifacts or meta data, is not possible. The customer can document changes by creating multiple independent files, while at the same time having mechanisms in place to detect duplicates and prevent them from being re-uploaded.

### 3.5. Annotation Creation / File Retrieval

The customer can configure annotations via API in order to retrieve a file at a later point from the archive. Annotations created and attached in the process of archiving a file. If annotations are set by the customer, the system validates the data transferred according to the annotation schema.

### 3.6. File size / Upload limit (fair use)

The maximum file size per export file is 10 MB. Larger export files are automatically rejected by the system without further notification and cannot be uploaded to fiskaly SAFE.

## 4. System requirements

- 4.1. The fiskaly SAFE service is a JSON-based RESTful Software-as-a-Service solution. A full documentation of the service is provided in the API description (<https://developer.fiskaly.com/api/safe/v1>) and integration guides are provided in the fiskaly developer page ([developer.fiskaly.com](https://developer.fiskaly.com)). A Quick-Start guide in the form of a Postman collection is also available.
- 4.2. Integration and operation of the service requires:
- a contractual relationship with fiskaly that permits the use of the service
  - an internet connection
  - an integration of the SAFE.API (whenever the customer want to access the service via API)
  - Configured fiskaly SIGN and/or DSFinVK services, if applicable

## 5. Security features

- 5.1. The customer is uniquely identified via the customer-specific API credentials they created during the integration of the API or via an authorized user at the fiskaly HUB. Access to all functional service endpoints apart from authentication is conditional upon the presence in the requests of a valid token created through these credentials.
- 5.2. All data provided by a fiskaly customer is property of that customer. No other customer has rights or possibility to view, retrieve or alter these data.



- 5.3. The data is stored on the fiskaly servers for as long as necessary to fulfill the contractual obligations and, if applicable, fiskaly's own legal retention obligations.
- 5.4. It is the customer's responsibility to secure access to their data on their end through appropriate user management and the application of up-to-date information security measures.

## 6. Maintenance and Support

- 6.1. fiskaly undertakes to maintain and regularly update the fiskaly SAFE service to ensure its security, availability, and compliance to the requirements issued by the national tax authorities.
- 6.2. The service shall be versioned according to semantic versioning. The initial LIVE version shall be 1.0.0. Significant changes to the functionality or nature of the service result in a new major release. All customer-facing changes shall be documented in a public changelog.
- 6.3. Maintenance activities may result in the temporary outage of the fiskaly SAFE service. As far as possible, these activities shall be announced at least two (2) weeks in advance so that customers may schedule their use of the service accordingly. Emergency maintenance activities may deviate from this. Customers are encouraged to refer and subscribe to the fiskaly status page (status.fiskaly.com) for relevant information.
- 6.4. fiskaly shall provide assistance to customers in the form of the fiskaly support portal (support.fiskaly.com). The portal hosts FAQs and how-to guides regarding all fiskaly services. The support team can be contacted via dev-support@fiskaly.com, or via Web Widget from the fiskaly fiskaly HUB, Support Page and Developer Page.

## 7. Testing

- 7.1. fiskaly provides a TEST environment for trying out the fiskaly SAFE service. This is a fully functional cloud-based storage with the same properties provided by the LIVE system. New versions of the service shall always be available on the TEST environment before their LIVE release.
- 7.2. fiskaly shall not be held responsible should real data be provided by the customer in the TEST environment.

## 8. Availability

- 8.1. fiskaly SAFE service is designed for high availability. As a rule, no data is lost even in the event of an incident. The recovery point objective (RPO) is a maximum of 5 seconds. fiskaly uses a synchronously replicating architecture and regularly audits its functionality. The Recovery Time Objective (RTO) is a maximum of 24 hours; full service is restored no later than 24 hours after the disruption occurs..

## 9. Integration and Compatibility

- 9.1. **Related to product option SAFE**
  - 9.1.1. SAFE is directly integrated into fiskaly HUB UI (starting with version 2.0).
  - 9.1.2. The activation or deactivation of the service is in the responsibility of the customer.
  - 9.1.3. SAFE is compatible with fiskaly SIGN and DSFinVK services.
- 9.2. **Related to product option SAFE flex**
  - 9.2.1. Integration of the SAFE API is the responsibility of the customer.
  - 9.2.2. The customers POS systems connect directly to the fiskaly SAFE API to transmit fiscal and fiscalization-related files for archiving. Users create an API key and authenticate it through the provided authentication endpoint. Once authenticated, an access token is issued, enabling file transmission to the archive, provided all

preliminary steps (e.g., creating annotations, configuring country-specific settings) are completed. This integration ensures data transmission and real-time archiving.

9.2.3. The individual documents are archived in separate “organizations” that represent a specific taxpayer or a specific business establishment. When uploading a file of type “Standardized Fiscal Data Export”, specific operations on the file are logged invariably (see below - audit security). Additionally, when uploading the file, customers will be asked to provide additional information annotations (annotations are metadata that are attached to content and instruct the filter on how to process or categorize it) are given.

9.2.4. To use the fiskaly SAFE API in a way that is compliant with the applicable laws, the following file types with the corresponding attributes of the respective annotation are mandatory:

- Standardized Fiscal Data export:
  - created\_at (created date of Document- Standardized Fiscal Data ZIP File),
  - retention\_period\_days (duration of storage of the document in accordance with legal requirements),
  - start\_date (start date of the exported data),
  - end\_date (end date of the exported data, may coincide with the start date),
  - client\_id (optional: List of Client IDs).
- TSS export
  - created\_at (document creation date),
  - retention\_period\_days (retention period of the document in accordance with legal requirements),
  - start\_date (start date of the exported data),
  - end\_date (end date of exported data, may coincide with start date),
  - tse\_id (ID of the TSS),
  - client\_ids (optional: List of Client IDs).

Additional annotations defined by the customer can also be saved to cover client-specific requirements for later searches.

9.2.5. Changes in applicable laws and regulations may result in significant changes to fiskaly SAFE service at any time. fiskaly will try to limit the impact of such changes on the service by bundling them into major releases. These releases will affect the API schema and will be reflected in the service URLs, e.g. v1 will be replaced by v2, etc. Resources created under the previous version(s) should not be affected, and will be available to the new major release, unless regulatory changes dictate otherwise. fiskaly will publish migration guides to inform and assist customers in transitioning to a new major release.

9.2.6. fiskaly aims to keep the number of major releases low, with at most one major release per year. However, as changes may reflect regulatory innovations that are time-critical, such a timeline may not be always possible. The release or deprecation of major versions shall be announced to all service customers well in advance.

## 10. User and Administration functions

### 10.1. Related to product option SAFE

- 10.1.1. Usage of SAFE is allowed on the basis of an authorized user in the fiskaly HUB.
- 10.1.2. Each authorized user has the right to:



- activate and configure the service via the UI of the fiskaly HUB.
- search and export, activate and configure the service via the UI of the fiskaly HUB.

#### 10.2. Related to product option **SAFE flex**

10.2.1. Usage SAFE flex is allowed on the basis of an authorized user in the fiskaly HUB.

10.2.2. Each authorized user has the right to:

- upload and manage all data required for the use of the service via the provided endpoints,
- export all data submitted via the provided endpoints.

10.3. No further administrative permissions are granted to a customer account. fiskaly reserves for itself the right to perform scheduled or ad hoc administrative or maintenance actions in order to:

- restore the correct behaviour of the service in case of malfunction,
- ensure the long-term stability and performance of the service,
- restrict customer access in case of non-compliance with contractual obligations,
- address customer requests.

### 11. Service Limitations

11.1. The fiskaly SAFE service facilitates the data collection in compliance with the applicable laws and regulations. As noted in Section 2.2, the fiskaly SAFE service does not provide any semantic validation of the data. The completeness and correctness of the data is the sole responsibility of the customer.

11.2. As noted, changes of the applicable laws and regulations may introduce breaking changes that will result in the deprecation of a major version of the fiskaly SAFE service. Customers are responsible for staying up to date with new fiskaly SAFE service major releases by taking steps to integrate them as soon as they are announced and made available in the TEST environment.

### 12. Customer obligations

In order to use fiskaly SAFE service compliant, the customer has the following obligations:

#### 12.1. Related to product option **SAFE**

- The customer is responsible to individually define the storage period for the artifacts.
- The customer is responsible for activation or deactivation of the service
- The customer is responsible configuring the service
- The customer is responsible to configure fiskaly SIGN and/or DSFinVK
- **Data provision:** The customer must transmit all required tax-relevant data to fiskaly in the format and schema specified by fiskaly (e.g. DFKA taxonomy for Germany) via the SAFE API.
- **Integration and ongoing transmission:** The customer is responsible for properly integrating the SAFE API into its POS system and ensuring that each relevant business transaction is transmitted to fiskaly SAFE in a timely and continuous manner.
- **Retrieval and verification obligations:** Exports generated by the customer via fiskaly SAFE (e.g. DSFinV-K files) must be retrieved and retained by the customer and submitted to the competent tax authorities if required.

#### 12.2. Related to product option **SAFE flex**

- The customer is responsible to individually define the storage period for the artifacts.

- The customer is responsible for exporting data from the Standardized Fiscal Data API (Standardized Fiscal Data Export).
- The customer is responsible to define the right granularity of the exported data (e.g. one export per TSS and day).
- The customer is responsible to configure the described annotations in order to use the fiskaly SAFE API in a way that is compliant with the applicable laws and regulations. There is no validation of the annotations selected and set by the customer.
- The customer is responsible to upload all relevant files provided by his POS system and with the correct annotations.
- The customer is responsible for properly integrating the SAFE API into their POS system and ensuring that every relevant business transaction is transferred to fiskaly SAFE promptly and continuously.
- Retrieval and proof requirements: Exports generated by the customer via SAFE (e.g., DSFinV-K files) must be retrieved by the customer, stored, and submitted to the relevant tax authorities upon request.