KassenSichV

What exactly is the cash register regulation (KassenSichV)?

The cash register regulation (KassenSichV) is a regulation effective 1 January 2020 for the implementation of new standards regarding the protection against manipulation of electronic recording devices (e.g. cash registers, electronic/computer-based cash register systems).

What is the purpose of the cash register regulation "KassenSichV"?

The objective of the cash register regulation "KassenSichV" is to detect subsequent manipulations of sales data. In order to effectively prevent manipulation of digital records of business transactions, the integrity, authenticity and completeness of the data must be ensured.

The tamper protection is essentially ensured by a so-called technical security system (TSE):

During the recording, the data is recorded and checked, processed in a specific format and by use of electronic signatures stored in a tamper-proof manner. The data can be exported at any time, so that you can quickly and easily provide all the necessary information to the tax authorities (cash register inspection).

Who is affected by it?

The KassenSichV primarily affects entrepreneurs who use the cash register and recording systems for the recording of business transactions. The KassenSichV applies to business transactions in which the seller's service is followed by payment (via cash, card payment, voucher), a quid pro quo of the customer - the so-called performance upon counter-performance.

The requirements apply to branches of foreign companies in Germany as well.[1]

[1] cf. Orientation guide for the application of § 146a AO (Fiscal Code) and the KassenSichV of the BMF (Federal Ministry of Finance; December 2019

Which recording systems are not affected?

- Ticket vending machines
- Ticket printers
- Electronic accounting programs
- Vending machines for goods and services
- ATMs
- Taximeters
- Odometers
- Gambling machines for money and goods[2]

Transitional periods

§ 146a AO (Fiscal Code) has been introduced by the law for protection against manipulations of digital basic recordings of December 22, 2016 (BGBI (Federal Law Gazette) p. 3152), according to which it is required that with the start of 1 January 2020, every electronic recording system used within the meaning of § 146a (1) clause 1 AO (Fiscal Code) in connection with § 1 clause 1 KassenSichV, as well as the therewith kept digital records, must be protected by a certified technical security system.

The technically required adjustments shall be carried out immediately and the legal requirements have to be met without delay as well. For the modification of a comprehensive upgrading of electronic recording systems within the meaning of § 146a AO (Fiscal Code), there will be no objection if these electronic recording systems do not have a certified technical security system by September 30 at the latest.[3]

BMF (Federal Ministry of Finance) deadline extension:

Cash registers that were purchased after November 25, 210 and before January 1, 2020 and which meet the requirements of the GoBD (the principles for properly maintaining, keeping and storing books, records and documents in electronic form and for data access, as provided by the German tax authorities) but cannot be upgraded and therefore do not meet the requirements of § 146a AO (Fiscal Code) may continue to be used until December 31, 2022.[4]

[2] cf. Provision for determining the technical requirements for electronic recording and security systems in business transactions (cash register regulation - KassenSichV) § 1 electronic recording system

[3] cf. Non-compliance regulation for the usage of electronic recording systems within the meaning of § 146a AO (Fiscal Code) without a certified technical security system after December 31, 2019

[4] cf. § 145a AO (Fiscal Code) Chapter 2.2.2

What do I have to do now as a cash register manufacturer?

The affected recording devices must be supplemented with a certified technical security system (TSE) with the effectiveness of the regulation as of 1 January 2020.

The technical security system consists of a security module, a memory for permanent storage of the data and a uniform digital interface (API). The technical security system is addressed by the electronic cash register system and assumes the protection of data. Each entry is thereby protected through electronic signatures. The secure records are permanently saved in a specified format.

The technical security system is therefore an addition to an already existing electronic cash register system.

As an A-Trust partner, you don't have to worry we offer an all-round carefree package:

Our solutions are easy to integrate and 100% legally compliant. The integration into your existing cash register system is possible without any problems, all of our solutions are open to all types of technologies - there are no restrictions regarding compatible cash register systems and no additional hardware is required.

What is a technical security system (TSE)?

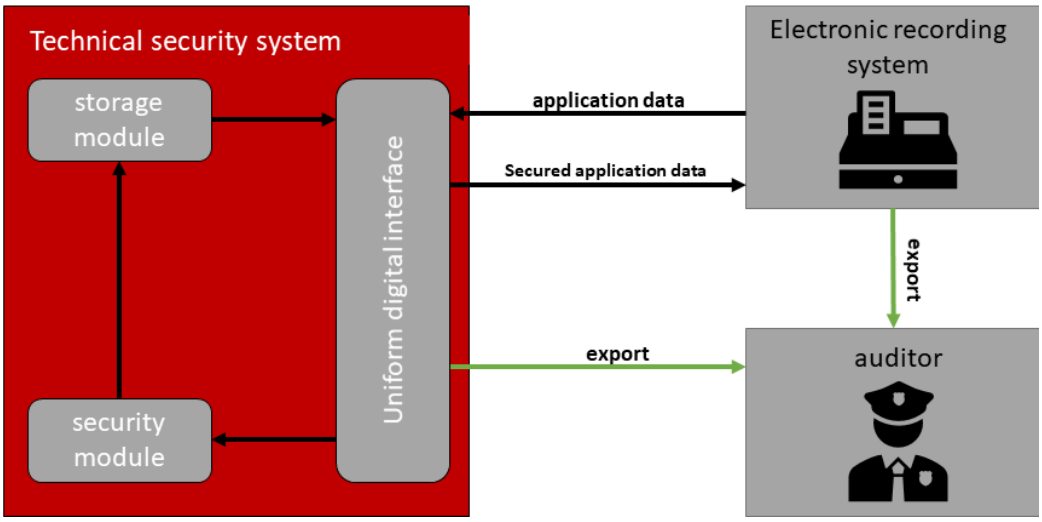
The technical security system (TSE) is the essential component for the achievement of anti-fraud protection and represents an addition to your cash register system, which is open to all types of technologies. The TSE consists of a uniform digital interface, a security module and a storage medium. The TSE receives data from the cash register system via the uniform interface. The security module supplements this data with further information and checks the related transaction data, protects and stores it in a uniform format in the storage medium and enables the data to be made available via the export interface in the event of an inspection by the tax authorities. In the event of a fault, the TSE also documents when the operation was interrupted and resumed.[5]

- The **uniform digital interface** consists of an export interface and an integration interface. The uniform digital interface is on one hand the link to the electronic recording device and ensures the receipt of the transaction data. On the other hand, the provision of the secured application data or system messages, audit data and the corresponding log data is ensured via TAR archives.[6]

[5] cf. Provision for determining the technical requirements for electronic recording devices and security systems in business transactions (cash register regulation - KassenSichV) § 5 Requirements to be met by the technical security system

[6] cf. KassenSichV § 4 Uniform digital interface

- The **security module** ensures the authentication of the data and the secure logging of the processes to be recorded. Among other things, it fulfills the functions of creating the log data, connecting and protecting the application and log data. The in this way secured application and log data form the basis for the data to be submitted in the event of an inspection.[7]
- The **storage medium** assumes the storage and provision of all secured data for the export in the event of a cash register inspection (Kassennachschau). With acloud-based solution, there are several implementations regarding the number of possible transactions.[8]



[7] cf. TR-03153. Page 25, Chapter 4, The security module
[8] cf. KassenSichV § 3 Storage of the basic recording

Certification of the TSE:

Manufacturers of a TSE must provide proof that the TSE is in compliance with the interoperability requirements of the technical guidelines. Proof must be provided by a certification of conformity according to the test specification TR-03153.

- **BSI TR-03153**

Furthermore, manufacturers of a TSE must provide proof that the security requirements are complied with. The evidence shall be provided by security certifications compliant to the common criteria with the following protection profiles:

- **BSI PP-SMAERS**
- **BSI PP-CSP** in the configuration according to the protection profile module CSP time stamp service and audit (PPM-TS-Au)[9]

A-Trust is currently under BSI (Federal Office for Information Security) certification process and is listed in the BSI homepage.

Our certification number is: **BSI-DSZ-CC-1140**

[9] cf. BSI (Federal Office for Information Security) - Frequently asked questions and answers (FAQ), Which certifications have to be successfully implemented to prove that a technical security system meets the requirements of the BSI?

What must be observed prior to the initial operation or the decommissioning of an electronic recording device?

Registration obligation for cash registers

Each cash register has a serial number. Taxpayers must register their cash register with the respective serial number with the tax authorities by 30 September 2020 at the latest. The BMF (Federal Ministry of Finance) leaves it up to the taxpayer to entrust this to tax consultants.

This means, that after the procurement of the electronic recording device a variety of information has to be provided to the responsible tax authorities, for the time being by use of an official form and in the future also electronically. The information must include the following items:

- Name and tax number of the taxpayer
- Type of TSE (BSI (Federal Office of Information Security) issued certification ID and serial number of the certified TSE)
- Type of electronic recording device used
- Number of electronic recording devices used per business location
- Serial number of the electronic recording device used
- Date of purchase or date of decommissioning of the electronic recording device used

The types of reporting are differentiated between registration, deregistration and correction. The electronic recording device that is registered by the taxpayer shall be clearly assigned to one business location. A separate notification has to be issued for each business location. However, several electronic recording devices can be covered within one business location in one notification. In the event of decommissioning, whereby loss is included as well, the same has to be reported by the taxpayer to the responsible financial authorities.[10]

[10] cf. Introduction of § 146a AO (Fiscal Code) by the law for protection against manipulation of digital basic records of December 22, 2016; application decree to § 146 AO (Fiscal Code), Chapter 9, June 17, 2019

Obligation to issue receipts

A receipt issuing obligation is provided for in § 146a AO (Fiscal Code). In the event that the TSE is unavailable, the obligation to issue receipts still applies - see TSE failure.

A receipt must include the following:

1.) Full name and complete address of the company;
2.) Issuing date of the receipt, the time of start of the process within the meaning of § 2, clause 2, number 1, and the time of the end of process within the meaning of § 2, clause 2, number 6;
3.) The quantity and type of items supplied or the scope and type of other services;
4.) The transaction number within the meaning of § 2, clause 2, number 2;
5.) The payment amount and the respective tax amount for the supply or other services shown as a total figure, as well as the applicable tax rate or, in the case of a tax exemption, the information that a tax exemption is applicable for the supply or other services;
6.) The serial number of the electronic recording device or the serial number of the security module.

The information on the receipt must be legible for anyone without mechanical assistance. A receipt can be issued on paper or electronically in a standardized data format with the consent of the recipient.[11]

DSFinV-K - digital interface of the financial administration for cash register systems

DSFinV-K 2.0 is the description of an interface for the export of data from electronic recording devices for data transfer in the context of external audits and cash register inspections. This shall ensure a uniform structure and description of files and data fields regardless of the electronic recording device used by the company. The company shall make the data available on a suitable data carrier in accordance with the conventions of the DSFinV-K 2.0.

The objective of DSFinV-K 2.0 is to define a data structure from electronic recording devices for which the use of the legally required uniform digital interface (§ 146a AO (Fiscal Code)) will apply as of January 1, 2020.

[11] cf. Provision for determining the technical requirement for electronic recording devices and security systems in business transactions (cash register regulation - KassenSichV) § 6 Requirements of the receipt

The following objectives shall be covered by the standardization:

- Uniform provision of data for the external audit as well as for cash register inspections through defined individual cash register transactions, master data and cash register balances, so that a progressive and retrograde verifiability between the basic records and the entry in the general ledger (financial accounting) is guaranteed.
- Enabling the transferring of all data recorded in the respective system to an archive system.
- Enabling a simplified verification of the structured cash register data transferred to the financial accounting.

Which data should be stored?

DSFinV-K (digital interface of the financial administration for cash register systems) specifies the data to be generated by the cash register. The two files associated with the TSE are specified in the A-Trust TSE example codes in the partner area:

- tse.csv
- transactions_tse.csv

Can the data be exported?

The A-Trust TSE solutions support the export of data in accordance with BSI (Federal Office for Information Security) TR-03151. Therefore, the data is exported in the format (TAR), which is required for the cash register inspection. The export functions offer the following filter options: by transaction number (from-to, or a specific number), by date, by client ID (a mere recording system) and combinations thereof.

What takes place during a cash register inspection (Kassennachschau) and how can I prepare myself?

Tax authorities are authorized to carry out a so-called "cash register inspection", i.e. an inspection of the respective recording device. The inspection of the cash register system takes place unannounced, but within the usual working hours. The inspectors must legitimize themselves with an official ID and should then be granted access to the cash register system. The correct operation of the electronic recording device is being checked. With the

effectiveness of the cash register regulation (KassenSichV), this also includes the operation of the technical security system (TSE).[12]

In order to be prepared for a cash register inspection, you should verify whether the receipts from the recording device (including the journal of the TSE) are provided in the required electronic format at all times. In addition, it is advisable to provide selected employees with the necessary access and usage rights and to familiarize the same with the recording device so that the inspection can also be carried out in the absence of the entrepreneur.

Failure of the TSE

In the event of a malfunction or failure of the technical security system, the same has to be documented accordingly (downtime and reason). In addition, the cash register users are obliged to promptly remedy the specific cause of failure.

If only the TSE has failed and the electronic recording device is working, further transactions can be carried out. The failure of the TSE must, however, be evident on the receipt (e.g. missing transaction number). The receipt issuance obligation continues to exist, even if not all data (e.g. transaction number) is available on the receipt.

In the event that the recording device fails as well, the recording may take place on paper during the malfunction. The downtimes are to be documented. In this case, there is no obligation to issue receipts.

Cash register users are obliged to immediately remedy the respective cause and, if possible, provide evidence thereof (e.g. invoice of repair).

Exemption from the obligation to issue receipts

In the event that only the printing or transmission unit of the electronic recording device fails, the recording device shall still be used. In this case, there is no obligation to issue receipts. Detailed information can be found under item 6 AEAO (Fiscal Code Application Decree) to § 146a.

[12] cf. Introduction of § 146a AO (Fiscal Code) by the law for protection against manipulation of digital basic records of December 22; Application Decree for § 146a AO (Fiscal Code), Chapter 4, Uniform interface for external tax audits and cash register inspections

Connection of the TSE to a cash register system

The TSE can be connected to the cash register system in different variants:

- **Cloud-TSE:** The SMAERS module communicates with the cloud on the cash register via the Internet.
- **USB stick/ SD card:** The TSE is connected directly to your cash register system via USB or SD slot.
- **Network-TSE:** If several cash registers are joined in one network, the A-Trust product **TSE-LAN** may be recommended. The **TSE-LAN** is integrated into your network to enable all cash registers to communicate in one place with a TSE.

Comparison of the TSE variants

	Online solution (Cloud TSE)	**Offline solution (stick/card)**
What does the TSE look like?	on top of the cloud, no hardware	USB stick or SD card, storage and security module
Installation	installation of SMAERS module on cash register	local installation
Where is the signature created?	In the cloud	on the USB stick/SD-card
How is the cash register connected to the TSE?	via Internet	with USB stick/SD card
Running costs	yes	no
Storage capacity	unlimited	until the memory on the USB stick/SD card is full
Location of signed receipts	in the cloud	on the TSE (Memory module)
Possible sources of faults for receipt signatures	cloud, Internet connection, cash register software	defective USB stick, cash register software
Loss of data	very low risk	loss of the TSE (USB stick)
Internet connection required?	yes	no
Internet outage	signing not possible	not affected

When must a technical security system be replaced?

The duration of the validity of A-Trust TSE certificates for technical security systems differs with the offline/online solutions.

- Certificates of the A-Trust **Online** solution are valid for 5 years.
- Certificates of the A-Trust **Offline** solution are valid for 5 1/2 years.

Certificates may be extended at any time.

There can be several reasons for the need to replace a technical security system:

➔ The certificate has expired
➔ The technical security system is defective - error message

Bibliography and further information

Which recording systems are not affected?

- Provision for determining the technical requirements for electronic recording devices and security systems in business transactions (cash register regulation - KassenSichV) § 1 Electronic recording devices

Transitional periods

- Non-compliance regulation for the usage of electronic recording systems within the meaning of § 146a AO (Fiscal Code) without a certified technical security system after December 31, 2019

What is a technical security system (TSE)?

- Detailed information can be found under § 5 KassenSichV (cash register regulation); 1.1, 3.2, 3.3, 4 – 7 BSI TR-03153; BSI TR-03151 SE API; 3 AEAO (Fiscal Code Application Decree) to § 146a.
- Uniform interface: Detailed information about the uniform digital interface can be found under § 4 KassenSichV; 3.2, 3.3, 3.4, 5 BSI TR03153; BSI TR-03151 SE; 4 AEAO (Fiscal Code Application Decree) to § 146a.
- Security module: Detailed information about the security module can be found under 3.2, 3.3, 3.5, 4 BSI TR-03153; 3 BSI TR-03151 SE API
- Storage module: Detailed information about the storage module can be found under § 3 KassenSichV; 3.2, 3.3, 6 BSI TR-03153; 4.5.3 BSI TR-03151 SE API; 8 AEAO to § 146a.

What must be observed prior to the initial operation or the decommissioning of an electronic recording device?

- Registration obligation for cash registers: More detailed information regarding the registration obligation can be found in item 9 of the application decree to § 146a of the tax code.
- Preparation of cash register inspection (Kassennachschau): Detailed information for the handling and function of the technical security system can be found under 4, 5 BSI TR-03151 SE API; and the detailed instruction for the check of the functionality of the technical security systemBSI TR-03151 TS, as well as information for the registration obligation §146a AO; 3.5 BSI TR-03153; BSI TR-03151 SE API; 2, 9 AEAO (Fiscal Code Application Decree) to § 146a.

What takes place at a cash register inspection (Kassennachschau)?

- Introduction of § 146a AO by the law for protection against manipulation of digital basic records of December 22; Application Decree for § 146a AO; Chapter 4, Uniform interface for external tax audits and cash register inspections

BSI (Federal Office for Information Security) - Frequently asked questions and answers (FAQ)

DSFinV-K 2.0 (Digital interface of the financial administration for cash register systems)