FEDERAL LAW GAZETTE
FOR THE REPUBLIC OF AUSTRIA

Year 2015 **Issued on December 11, 2015** **Part II**

410th Regulation: Cash Register Security Regulation, [RKSV]

410th Regulation by the Federal Minister of Finance on the technical details for security devices in cash registers and other measures used for data security (Cash Register Security Regulation, [RKSV])

Based on Sections 131b Para. 5 Clause 1, 3 and 4 and Section 132a Para. 8 of the Federal Tax Code [BAO], Federal Law Gazette [BGBl.] No. 194/1961, last amended by the Federal Law Federal Law Gazette [BGBl.] I No. 118/2015, it is decreed:

Table of Contents

Chapter 1
General Part

Area of Application

§ **1.** The Cash Register Security Regulation regulates

1. the technical features of the following that are required for the technical implementation of the protection against manipulation of electronic recording systems
   a) of the cash register,
   b) of the signature creation unit,
   c) of the communication between cash register and signature creation unit,
2. the additional requirements of the receipt pursuant to § 132a Para. 8 of the – Federal Tax Code[(BAO], Federal Law Gazette [BGBl.] No. 164/1961,
3. details about the issuing of notices of assessment with regard to closed overall systems and
4. the access by authorities to the necessary data for purposes under supervisory and tax law.

References to Persons

§ 2. All references made in this regulation to persons apply equally to men and women.

Abbreviations and Definitions of Terms

§ **3.** Pursuant to this regulation, the following terms are defined as indicated:

1. AES-256: encryption procedure pursuant to the Advanced Encryption Standard (AES FIPS 197 11/26/2001) with a key length of 256 bit
2. Barcode: standard “Code 128”, defined in ISO/IEC 15417:2007
3. Cash transaction: transactions pursuant to § 131b Para. 1 Clause 3 of the Federal Tax Code [BAO]
4. Database about security devices in cash registers: database of the Federal Ministry of Finance in which the data named in § 18 Para. 2 with regard to the security devices in cash registers and checks by the security devices are recorded
5. Data collection protocol [DEP]: an event log file integrated in the memory of the cash register or in an external memory that documents the cash transactions with receipt content completely and chronologically in a continuous manner in real time in each case with creation of receipt
6. Input station: device for the recording of cash transactions that is connected to a cash register in particular for the signing and documentation of the cash transactions
7. Electronic recording: complete documentation of cash transactions continuously and chronologically in electronic form
8. Electronic (cryptographic) signature: electronic data that are attached to other electronic data or are logically linked with these and that are used for authentication pursuant to § 2 Clause 1 of the Signature Act – [SigG], Federal Law Gazette [BGBl.] I No. 190/1999
9. FinanzOnline: electronic procedure of the tax authority pursuant to the 2006 FinanzOnline Regulation, Federal Law Gazette [BGBl.] II No. 97/2006, in the respectively valid version

10. Closed overall system: electronic recording system in which enterprise resource planning, accounting and till systems are seamlessly connected with one another and that is connected to more than 30 cash registers
11. Global Location Number (GLN): reference number issued by Bundesanstalt Statistik Österreich [Federal Institute Statistics Austria] under the name "secondary ID"
12. Hardware security module (HSM): signature creation unit that is used to create (qualified) electronic signatures and is used in particular with server-based solutions
13. Homepage of the Federal Ministry of Finance [BMF]: www.bmf.gv.at
14. Till identification number: code of a cash register reported via FinanzOnline and that also facilitates a differentiation of various cash registers with the same signature creation unit
15. Machine-readable code: input value for OCR, barcode or QR code representation
16. Monthly counter: totalizing memory in the cash register that records the interim statuses of the sales counter as of the end of the month
17. Object Identifier (OID): globally unique designator pursuant to ISO/IEC 9834-1 and A 2642 that is used to name an information object. The OID is used in this regulation in order to restrict the use of the signature certificate pursuant to § 5 Para. 1 Clause 8 [SigG] in the respectively valid version to the purpose 'Austrian finance administration cash register owner'
18. Optical Character Recognition (OCR): Standard OCR-A, defined in ISO 1073-1:1976
19. Contractor's reference number: a key known to the tax authority to identify the contractor (tax number, VAT ID number, GLN)
20. QR code: Two-dimensional symbol pursuant to JIS X 0510/2004 standard
21. Cash register (also electronic cash register): generalized form of any electronic data processing system that creates electronic records to determine a solution and document individual cash transactions, in particular electronic cash registers of any design, server-based recording systems (also to handle online transactions), scales with till functions and a taximeter. A cash register can be connected with input stations
22. Serial number of the signature certificate: a unique code for the certificate issued by the certification services provider and included in the certificate to make it easier to find the certificate in the directory of the certification service provider (CSP)
23. Secure signature creation unit: configured software or hardware that is used to process the signature creation data and that corresponds to the security requirements of the SigG and the regulations issued on this (§ 2 Clause 5 SigG)
24. Signature test data: data such as codes or public signature keys that are used to check an electronic signature (§ 2 Clause 6 SigG)
25. Signature value: electronic value of the signature determined within the framework of the signature creation
26. Start receipt: first receipt that is created using a cash register identification number and ensures the complete chaining of all receipts generated and saved under this cash register identification number
27. Totalizing memory: memory in the cash register that reflects the interim or a current final status of all accumulated amounts
28. Trust list (trustworthy list pursuant to the decision by the Commission 2009/767/EC about measures to make the usage of electronic procedures about uniform contact persons pursuant to the directive 2006/123/EC regarding services in the internal market, OJ No. L 274 dated 10/20/2009 p. 36): list of the certification service providers (CSPs) for qualified certificates to be kept by all Member States pursuant to the obligations from Article 2 of the decision 2009/767/EC
29. Sales counter: totalizing memory in the cash register that adds up the cash transactions of the cash register on a continuous basis
30. Verification: checking of signed data for integrity and authenticity, that the data are signed after the signature creation by the correct signature creation unit and are not changed
31. Payment receipt (receipt): confirmation with certain formal content, which documents the fundamental content of the legal transaction between the business partners in paper or electronic form and is handed over or communicated in electronic form on payment

32. Certificate: an electronic certificate with signature test data are assigned to a certain person and their identity is confirmed pursuant to § 2 Clause 8 SigG
33. Certification service provider (CSP): organization that issues certificates or provides other services in connection with electronic signatures pursuant to the directive 1999/93/EC regarding community boundary parameters for electronic signatures, OJ No. L 13 dated 01/19/2000 p. 12.

Chapter 2
Technical Regulations

Section 1
General

Description of the Security Device

§ 4. (1) Pursuant to § 131b Para. 2 of the Federal Tax Code [BAO], the security device consists of a chain of the cash transactions with the aid of the electronic signature of the signature creation unit.

(2) The chain is formed by including elements of the last assigned signature stored in the data collection protocol in the current signature to be created. In the creation of the first cash transaction, the last assigned signature is replaced by the till identification number.

Section 2
Requirements of the Cash Register

General Requirements

§ 5. (1) Each cash register must have a data collection protocol and a printer for the creation or a device for the electronic transmission of payment receipts.

(2) Each cash register must have a suitable interface to a security device with a signature creation unit. Several cash registers can also be connected with a signature creation unit.

(3) Each cash register must be equipped with the freely available encryption algorithm AES 256 in order to be able to carry out the encryptions necessary for the machine-readable code.

(4) Each cash register must be assigned a unique cash register identification number in the company.

(5) The cash register may not contain any devices via which the control of the security device can be circumvented.

(6) The usage of a cash register by several contractors is only permissible subject to the requirement that each contractor can use a certificate assigned to it and the cash register can keep a special data collection protocol for each contractor.

Putting into Operation of the Security Device for the Cash Register

§ 6. (1) The putting into operation of the security device for the cash register consists of the setting up of the data collection protocol (§ 7) and the filing of the cash register identification number as part of the data of the first cash transaction to be signed with the amount zero (0) in the data collection protocol.

(2) Before January 1, 2017, the security device pursuant to Para. 1 can already be put into operation before the registration (§ 16). Registration must have been done by January 1, 2017.

(3) If registration is done after December 31, 2016, the putting into operation has to be done within a week after registration of the signature creation unit (§ 16).

(4) Before putting the security device into operation, the contractor has to check the creation of the signature (§ 9 Para. 3) and the encryption of the sales counter (§ 9 Para. 2 Clause 5) with the aid of the start receipt. If the creation of the signature and/or the encryption of the sales counter does not correspond to the requirements of § 9, the cash register is to be treated directly as a cash register with a failed signature creation unit pursuant to § 17 Para. 4. The test result is to be documented and stored with the printed start receipt pursuant to § 132 of the Federal Tax Code [BAO].

Data Collection Protocol

§ 7. (1) Each cash register has to keep a data collection protocol in which each individual cash transaction is to be recorded and saved. At least the receipt data pursuant to § 132a Para. 3 of the Federal Tax Code [BAO] are to be recorded for each cash transaction.

(2) Training and cancellation bookings are to be recorded as cash transactions and saved in the data collection protocol.

(3) The data of the data collection protocol are to be backed up in unmodified form at least every quarter on an electronic external medium. This back-up is to be stored pursuant to § 132 of the Federal Tax Code [BAO].

(4) The content of the machine-readable code (§ 10 Para. 2) of the cash transactions are to be recorded in the data collection protocol of the cash register together with the respective cash transactions.

(5) From January 1, 2017, it must be possible to export the data collection protocol of a cash register at any time onto an external data carrier in the export format data collection protocol according to clause 3 of the **Appendix**.

Totalizing Memory

§ 8. (1) The cash transactions recorded in the cash register are to be continuously added up (sales counter). Training bookings may not have an impact on the sales counter.

(2) At the end of each month, interim statuses of the sales counter are to be determined (monthly counter) and saved as a cash transaction with the amount zero (0) and electronic signature of the signature creation unit (monthly receipt) in the data collection protocol of the cash register.

(3) With the expiry of each calendar year, the monthly receipt that contains the counter status at the end of the year (yearly receipt) is to be checked and stored pursuant to § 132 of the Federal Tax Code [BAO]. § 6 Para. 4 is to be applied in an analogous manner when checking the annual receipt.

Signature Creation by the Signature Creation Unit

§ 9. (1) To guarantee protection against manipulation pursuant to § 131b Para. 2 of the Federal Tax Code [BAO], it must be possible for electronic signatures to be requested and taken over by the cash register via a suitable interface to the signature creation unit. Each individual cash transaction and monthly, yearly and final receipt as well as each training and cancellation booking are to be signed electronically.

(2) The following data are to be included in the signature creation:

1. till identification number
2. sequential number of the cash transactions
3. date and time of receipt issuing
4. amount of the cash payment separated according to tax rates pursuant to § 10 of the 1994 VAT Act
   – [UStG 1994], Federal Law Gazette [BGBl.] No. 663/1994 in the respectively valid version
5. with the encryption algorithm AES 256 according to Clause 8 and Clause 9 of the **Appendix** encrypted status of the sales counter
6. serial number of the signature certificate
7. signature value of the previous cash transaction of the data collection protocol (chaining value according to Clause 4 of the **Appendix**)

(3) The prepared data (Para. 2) have to be automatically electronically signed by the signature creation unit pursuant to the signature format according to Clause 4 and Clause 5 of the **Appendix**.

(4) The signature reported by the signature creation unit in the result format of the signature creation according to Clause 6 of the **Appendix** is to be printed on the respective receipt pursuant to the specifications of § 10 as part of the machine-readable code and to save it permanently in the data collection protocol with the receipt data according to Clause 11 of the **Appendix** (§ 7 Para. 4).

Preparation of the Machine-Readable Code

§ 10. (1) After each signature value has been determined, the cash register has to prepare a machine-readable code according to Clause 12 of the **Appendix** for the creation of the receipt and the saving in the data collection protocol.

(2) The machine-readable code has to include the following data:

1. Till identification number
2. Sequential number of the cash transactions
3. Date and time of receipt issuing

4. amount of the cash payment separated according to tax rates
5. with the encryption algorithm AES 256 according to Clause 8 and Clause 9 of the **Appendix** encrypted status of the sales counter
6. serial number of the signature certificate
7. signature value of the previous cash transaction of the data collection protocol (chaining value according to Clause 4 of the **Appendix**)
8. signature value of the respective cash transaction.

(3) Training and cancellation bookings also have to contain the designation "training booking" or "cancellation booking" in the machine-readable code.

Document Creation

§ 11. (1) In addition to the receipt data pursuant to Section 132a Para. 3 of the Federal Tax Code [BAO], the following data have to be indicated on the receipt:

1. till identification number
2. date and time of receipt issuing
3. amount of the cash payment separated according to tax rates
4. content of the machine-readable code.

(2) If a machine-readable code cannot be printed on the receipt as a QR code, the data pursuant to Para. 1 are to be provided either

1. as a link dependent on the signature value of the respective cash transaction in machine-readable form as a barcode or OCR to retrieve the data or to be indicated on the receipt or
2. to be indicated on the receipt in accordance with the coding defined in Clause 14 of the **Appendix**.

(3) Receipts for training and cancellation bookings are to be explicitly marked as such.

Section 3
Requirements of the Signature Creation Units

General Requirements

§ 12. The technical requirements of the signature creation unit correspond to the requirements of signature creation units for qualified signatures pursuant to Section 18 SigG in the respectively valid version and pursuant to Section 6 of the 2008 Signature Regulation – SigV 2008, of the Federal Law Gazette [BGBl.] II No. 3/2008, in the respectively valid version. Instead of the test envisaged in Section 6 Para. 3 last sentence of the 2008 SigV, a test can take place with regard to the content-related requirements of the Cash Register Security Regulation, whereby the requirement of the sole control and its impact on the operation is not the subject of this test due to the chaining.

Signature Key Pair and Signature Creation

§ 13. With regard to applicable signature algorithms and keys, the regulations of SigV 2008 regarding the algorithms and parameters for qualified signatures from the Appendix to SigV 2008, points 1 to 7 "Algorithms and parameters for qualified electronic signatures" are to be applied.

Verifiability of the Signatures

§ 14. The signature value of the respective cash transaction must be verifiable based on the machine-readable code indicated on the receipt. For this purpose, in particular the data contained in Section 10 Para. 2 must be included on the receipt. The pre-processing of the data included for this purpose in compressed form in machine-readable code has to be done pursuant to Clause 13 of the **Appendix**.

Chapter 3
Procurement and Registration of the Signature Creation Unit; Control

Procurement of the Signature Creation Unit

§ 15. (1) Contractors that are subject to the cash register obligation pursuant to Section 131b of the Federal Tax Code [BAO] have to acquire the necessary number of signature creation units from a certification services provider that is domiciled in the EU/EEA area or in Switzerland and that offers qualified signature certificates. The costs for the procurement of the signature creation unit are to be borne by the contractor.

(2) To acquire the signature certificate, the contractor has to have a reference number assigned to the contractor and known to the tax authority and as a value of the OID "Austrian Finance Administration Cash Register Owner" (Clause 16 of the **Appendix**) pursuant to the proviso of § 5 Para. 1 Clause 8 SigG entered in its signature certificate.

(3) The certification services provider awards a signature certificate for each signature creation unit and the certificate contains the following information:

1. type and value of the contractor's reference number assigned to the signature creation unit,
2. serial number of the signature certificate and
3. start and end of the validity of the certificate.

A use of the certificate beyond the end of its validity is permissible if the signature algorithm existing in the certificate pursuant to Clause 2 of the **Appendix** is seen as secure.

Registration of the Signature Creation Unit

§ 16. (1) The contractor or its authorized party representative has to report the acquisition of its signature creation unit via FinanzOnline. In the process, the serial number of the signature certificate, the type of the signature creation unit and the cash register identification numbers of the cash registers to be connected with the signature creation unit are to be announced. In addition, the contractor has to announce the freely selectable user key for the decryption (Clause 8 of the **Appendix**) of the data encrypted with the encryption algorithm AES 256 in machine-readable code via FinanzOnline. If the reporting via FinanzOnline cannot reasonably be expected of the contractor due to a lack of technical prerequisites, the reporting is to be done using the official template.

(2) Only after checking whether the CSP exists in the public trust list and the signature certificate exists in the directory of the CSP for each reported signature creation unit under the indicated serial number of the signature certificate and the valid reference number of the contractor, will these data be transferred to the database for security devices in cash registers (§ 18).

Announcement of the Deactivation of the Security Device for the Cash Register

§ 17. (1) The contractor or its authorized party representative has to notify via FinanzOnline or the tax office responsible for collecting the sales tax, any failure that is not just temporary and any deactivation of the security device in the cash register in the event of

1. theft or other loss of the signature creation unit or cash register,
2. loss of function of the signature creation unit or cash register or
3. deactivation of the signature creation unit or cash register

without unnecessary delay.

(2) For this purpose, the contractor has to provide the following information:

1. description of the respective components of the safety device
2. reason for the failure or the deactivation
3. start of the failure or the deactivation.

(3) All failures and deactivations reported via FinanzOnline that are not just temporary are noted in the database on safety devices for the cash registers.

(4) With each failure of the signature creation unit, the cash transactions are to be recorded on another cash register that has an existing connection to a signature creation unit. If this should not be possible, when preparing and using the machine-readable code (§ 10), the contractor has to use the string of characters "safety device failed" instead of the signature value of the respective cash transaction (Section 10 Para. 2 Clause 8) in the result of the signature creation according to Clause 6 of the **Appendix**. The note "security device failed" is also to be attached so that it is clearly visible on the receipt (§ 11). After the recommissioning of the signature creation unit, a signed collected receipt with the amount zero (0) is also

to be created for the receipts that were given the note "security device failed" during the respective failure and this is to be saved in the data collection protocol.

(5) With each failure of a cash register, the cash transactions are to be recorded on other cash registers. If this should not be possible, the cash transactions are to be recorded manually and duplicates of the receipts stored. After the correction of the fault, the individual transactions are to be subsequently recorded based on the stored

duplicates and the duplicates of these payment receipts stored (§ 132 of the Federal Tax Code [BAO]).

(6) If after the failure of a cash register, a new data collection protection has to be set up, the signature value of the last available cash transaction or the signature value of the start receipt in the data collection protection is to be used as a signature value of the previous cash transaction (§ 10 Para. 2 Clause 7). The end of the failure or the deactivation is to be announced via FinanzOnline. If the reporting via FinanzOnline cannot reasonably be expected of the contractor due to a lack of technical prerequisites, the reporting is to be done using the official template.

(7) If a recommissioning of the signature creation unit (Para. 4) is no longer possible, the contractor has to procure a new signature creation unit (§ 15), register it (§ 16) and carry out a new commissioning of the security device pursuant to § 6 Para. 1 to 4. If the last cash transaction made can be determined from the data collection protocol, the commissioning of the security device pursuant to § 6 Para. 1 to 4 is no longer necessary and the provisions regarding the collective receipt of Para. 4 apply. Cash transactions recorded manually during the failure are to be subsequently recorded at any rate.

(8) In the case of a scheduled deactivation of the cash register (Para. 1 Clause 3), the contractor has to create a final receipt with the amount zero (0). The final receipt is to be printed out and stored pursuant to § 132 of the Federal Tax Code [BAO].

Database on Safety Devices for the Cash Registers

§ 18. (1) For the internal documentation of the signature creation units assigned to a contractor, the Federal Minister of Finance keeps a database about security devices for the cash registers.

(2) This contains the following data:

1. Name of the contractors
2. Key of the contractors
3. Type of the security device
4. Serial numbers of the signature certificates
5. Identification numbers of the cash registers
6. Number of the cash registers connected to the security devices
7. User key for the decryption of the data encrypted with the encryption algorithm AES 256
8. Date of registration
9. Start and end of failures or deactivations of the security devices
10. Components affected by failures or deactivations of the security devices
11. Reason for the failure or the deactivation of the security devices
12. Data from checks.

(3) The Federal Minister of Finance is the client under data protection law pursuant to § 4 Clause 4 of the 2000 Data Protection Act – [DSG 2000], Federal Law Gazette [BGBl.] I No. 165/1999, for the database on security devices for cash registers. It must guarantee its set-up and operation. Bundesrechenzentrum Gesellschaft mit beschränkter Haftung [BRZ GmbH] is the statutory service provider for the database on security devices for cash registers pursuant to § 4 Clause 5 and § 10 Para. 2 DSG 2000.

Control and Testing of the Data Security for Cash Registers

§ 19. (1) At the request of the bodies of the tax authority, the contractor has to record a cash transaction with an amount zero (0) and hand over the receipt produced by the cash register for control purposes. With cash registers with a device for the electronic communication of payment receipts, the receipt is to be provided in electronic form.

(2) At the request of the bodies of the tax authority, the contractor must export and hand over the data collection protocol for a period specified by the body of the tax authority on an external data carrier. The data carrier is to be provided by the contractor.

Chapter 4
Closed Overall Systems

Technical and Organizational Requirements

§ 20. (1) The protection against manipulation in closed overall systems pursuant to § 131b Para. 4 of the Fiscal Tax Code (BAO) is to be guaranteed by a security device that consists of a chaining of the bar transactions with the aid of the prepared data pursuant to § 9 Para. 2 in the signature format according to Clause 4 and 5 of the **Appendix**.

(2) This regulation applies for closed overall systems with the exception of §§ 5 Para. 2, 12, 15 and 17 Para. 4. §§ 4 Para. 1, 6 Para. 4, 8 Para. 2, 9, 16 Para. 1 and 2, 17 Para. 1 to 3, 17 Para. 7 and 18 and the **Appendix** are to be applied with the proviso that neither a signature creation unit nor a signature certificate are required and that also several cash registers with a common data collection protocol can be assigned to one till identification number. Para. 4 remains unaffected by this.

(3) With closed overall systems, the reference number of the contractor is to be used instead of the signature certificate (§ 9 Para. 2 Clause 6 and § 10 Para. 2 Clause 6). The reference number of the contractor may have to be supplemented by suitable additions (e.g. numbers to facilitate unique signature test data. In the database pursuant to § 18, the signature test data are to be recorded instead of the serial number of the signature certificate. The reference number of the contractor and the signature test data must be indicated in the expert report pursuant to § 21.

(4) Only contractors who use a closed overall system as an electronic recording system that is connected to more than 30 cash registers are authorized to apply pursuant to Section 131b Para. 4 of the Federal Tax Code [BAO].

Expert Assessment of Closed Overall Systems

§ 21. (1) During the assessment of closed overall systems, the following checks in particular are to be carried out:

1. the existence of a closed overall system,
2. the existence of the technical and organizational requirements for the protection against manipulation of the closed overall system.

(2) In the expert report, in particular all software components necessary for the operation of the security device of the closed overall system pursuant to § 20 Para. 1 are to be indicated and test reports for these components attached. The software components are to be signed with the mathematical hash function Secure Hash Algorithm (SHA-256) with a start value that corresponds to null (0000 0000 0000 0000) for subsequent verification. It must be indicated in the test reports in a transparent manner how the individual components are tested. The protection against manipulation and equivalence with regard to security with a signature creation unit are to be confirmed. An organizational chart with all hardware and software components and data memory of the closed overall systems and an overview of the processing procedures that take place automatically are to be attached to the expert report.

(3) The expert report also has to include information on what organizational measures are envisaged for the ongoing check of the protection against manipulation. In the process, it is to be depicted in particular which operational functions in the company’s organizational structure are endowed with which access and intervention rights that can bring about changes to the total system, that access is logged and through which measures the protection against manipulation of the closed system is checked on an ongoing basis. In addition, it is to be shown how, in the event of a system failure, the individual recording obligation, the back-up of the till sales and the issuing of receipts is guaranteed in a legally compliant manner (failure plan).

(4) It is to be assessed in the expert report whether the closed overall system meets the requirements of § 20 Para. 1 and 2 and whether the technical and organizational back-up measures of Para. 2 and 3 are met.

(5) If several contractors that are economically linked via a vertical distribution system or through merchandise or service franchising or a part of a Group pursuant to § 244 of the Enterprises Code (UGB) jointly use a closed overall system with more than 30 cash registers in total and if the expert report assesses the protection against manipulation of this system for these contractors, this expert report can be used as a basis by several contractors for their application for the issuing of an assessment notice. Para. 3 is to be applied in an analogous manner for all users of the closed overall system. Deliveries and other services that are made outside of the closed

overall system in the company concerned are not covered by the validity of the notice of assessment.

(6) Only experts sworn by the court may be commissioned with the creation of such reports. The completeness of the security-relevant checks in the expert report is to be certified by a confirmation center pursuant to § 19 SigG.

(7) The costs for the creation of the expert reports will be borne by the contractor.

Notice of Assessment

§ 22. (1) In the notice of assessment from the tax authority pursuant to § 131b Para. 4 of the Federal Tax Code [BAO], the software components of the security device pursuant to § 20 Para. 1 forming the basis for the expert report are to be identified with the aid of the software signature (§ 21 Para. 2).

(2) Closed overall systems confirmed with the notice of assessment are registered in the database on security devices (§ 18).

(3) If the protection against manipulation of the closed overall system cannot be confirmed by the tax office, the contractor is to be granted a one-off subsequent period of one month for the subsequent implementation of the measures guaranteeing the protection against manipulation, furnishing an expert report confirming these measures. In this case, the tax office has to decide this on the basis of these facts.

(4) If the protection against manipulation of the closed overall system is not confirmed with the legally valid assessment of the tax office, the contractor has to effect the protection against manipulation within three months from occurrence of the legal validity, using a signature creation unit (§ 131b Para. 2 of the Federal Tax Code [BAO], otherwise the obligations pursuant to § 131b Para. 2 of the Federal Tax Code [BAO] will not apply on expiry of this deadline.

Change in the Actual Circumstances

§ 23. (1) Changes to the closed overall system confirmed with the notice of assessment are to be reported to the tax office responsible for collecting the VAT before their implementation, under submission of a new expert report (§ 21) if a comprehensive changeover of the closed overall system (e.g. change in technology) or a change in the software components of the security device pursuant to § 20 Para. 1 is planned or the application requirements pursuant to §§ 20 Para. 4 or 21 Para. 2 are no longer met. Such changes to the closed overall system are to be agreed with the notice of assessment.

(2) These intended changes are to be reported via FinanzOnline.

(3) If the contractor becomes aware of facts after the notice of assessment has been issued that give rise to doubts regarding the protection against manipulation of the closed overall system, it must report this via FinanzOnline without any unnecessary delay.

Control of the Identity of the Software Component Pursuant to § 21 Para. 2

§ 24. The bodies of the tax authority are entitled to check the compliance of the software component pursuant to § 21 Para. 2 with the software component in use in the closed overall system. For this purpose, the closed overall system must provide an input option of a start value for the local request of the software signature value and calculate and display the software signature value of the component.

Chapter 5
Final Provisions

Entry into Force

§ 25. (1) The Regulation enters into force on January 1, 2017.

(2) In deviation from Para. 1, § 1 to 3, § 5 Para. 1, § 7 Para. 1, § 17 Para. 5 and § 19 Para. 2 enter into force on January 1 2016.

(3) In deviation from Para. 1 and 2, § 6, § 15, § 16, § 18, § 21 and § 22 enter into force on July 1, 2016.

(4) This regulation was notified pursuant to the directive 98/34/EC regarding information procedure in the field of standards and technical regulations and the regulations for the services of the Information Society, OJ No. L 204 dated 07/21/1998, p. 37, last amended by the regulation (EU) no. 1025/2012 on European standardization, on the amendment of the directives 89/686/EEC and 93/15/EEC and the directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC,

2007/23/EC, 2009/23/EC and 2009/105/EC and on the rescission of the decision 87/95/EEC and of the decision No. 1673/2006/EC, OJ no. L 316 dated 11/14/2012 p. 12, at the European Commission under the notification number 2015/515/A.

Schelling