# Report and Software Certification on the Audit of the Archiving Software FileLock Version 2.3

GRAU DATA AG
Schwäbisch Gmünd

# Table of contents


| | | |
|---|---|---|
| **1** | **Contents and performance of the engagement** | **1** |
| 1.1 | Audit engagement | 1 |
| 1.2 | Auditing Standards | 2 |
| 1.3 | Engagement terms | 3 |
| 1.4 | Procedure for the assessment of conformity with the regulations | 3 |
| 1.5 | Requirements of commercial and tax law | 4 |
| 1.6 | Procedure and extent of the audit | 5 |
| 1.7 | Disclosure of the software certification | 7 |
| 1.8 | Special Considerations | 8 |
| **2** | **Audit results** | **9** |
| 2.1 | Summary of the audit results | 9 |
| 2.2 | Software Certification | 10 |
| **3** | **Performance of the audit and results in detail** | **12** |
| 3.1 | Review and introduction to the software product | 12 |
| 3.1.1 | General | 12 |
| 3.1.2 | Range of functions | 12 |
| 3.1.3 | Description of the test environment used | 13 |
| 3.1.4 | Audit of the process documentation | 13 |
| 3.2 | Assessment of the software development procedure | 14 |
| 3.3 | Audit of the software security functions | 15 |
| 3.3.1 | Administration | 15 |
| 3.3.2 | Data backup and recovery procedure | 17 |
| 3.4 | Audit of the appropriateness and functionality of the program functions | 18 |
| 3.4.1 | Archiving | 18 |

**Appendix** General Engagement Terms

# 1 Contents and performance of the engagement

## 1.1 Audit engagement

The management of

**GRAU DATA AG, Schwäbisch Gmünd**

– also referred to hereinafter as the "company" or "GRAU DATA" for short –

engaged KPMG AG Wirtschaftsprüfungsgesellschaft, Frankfurt am Main – referred to hereinafter as "KPMG" for short –

on 14 August 2014 to audit the compliance of version 2.3 of the FileLock standard archiving software in accordance with auditing standard IDW PS 880 of the Institut der Wirtschaftsprüfer, "Audit of Software Products".

On account of the functions of the software, the assessment was carried out essentially on the basis of IDW Accounting Practice Statement: Principles of Proper Accounting when Using Electronic Archiving Procedures" (IDW RS FAIT 3). In this process, it was audited whether, when used properly, the software allows electronic archiving for the long-term and unalterable storage of accounting-related documents on machine-readable data storage media in fulfilment of the legal retention duties pursuant to Section 257 of the Handelsgesetzbuch [HGB – German Commercial Code]. Furthermore, the regulations in Austria in the form of Section 132 of the Austrian Bundesabgabenordnung [BAO – Federal Fiscal Code] and in Switzerland in the form of the Swiss Obligationenrecht [Code of Obligations] in conjunction with the Geschäftsbücherverordnung [GeBüV – Business Records Ordinance] as of 1 January 2013 were also taken into consideration.

With FileLock, GRAU DATA offers a product with which data files can be archived in unalterable form on existing storage systems.

The subject matter of the service performed by KPMG was the audit of the FileLock software in the version currently distributed in terms of the unalterable storage of data on various storage media in accordance with the German IDW audit standards "Audit of Software Products" (IDW PS 880). The objective of the software audit was to assess compliance with the generally accepted accounting principles in terms of the archiving procedure defined by the software for Germany, Austria and Switzerland. KPMG audited whether the software allows the completeness of the processing when it is used properly.

## 1.3 Engagement terms

The terms governing our engagement are set out in the General Engagement Terms [GET] for Auditors and Auditing Firms as amended on 1 January 2002 and attached in the appendix, which also define our liability to third parties. In addition to the maximum indemnity amount of EUR 4 million specified in no. 9 Section 2 clause 1 of the GET, we are liable to the amount of EUR 5 million specified in no. 9 Section 2 clause 5 of the GET in respect of damages caused by negligence. Broadening of liability shall not apply to damages for which a maximum indemnity is regulated by law.

Furthermore, the engagement is subject to the above-mentioned GET with the provision that the maximum indemnity limits contained therein apply jointly to all persons who receive this audit report with our prior consent.

By acknowledging and using the information contained in this report, each recipient confirms that they have taken note of the regulations stipulated there (including the regulation on liability under no. 9 of the GET) and recognises their validity in relationship to us.

## 1.4 Procedure for the assessment of conformity with the regulations

In the context of this report, exclusively the requirements for archiving that is tamper-proof/in compliance with the GAAP form the basis for the assessment of whether FileLock is in conformity with the regulations.

The requirements for tamper-proof (also GAAP-compliant) archiving are derived from the regulations and interpretations of the Commercial Code (HGB) and the Fiscal Code (AO) in Germany as well as the Swiss Code of Obligations (GeBüV) and the Austrian Federal Fiscal Code (BAO) and stipulate verifiable compliance with the requirements for an internal control system (ICS), which are defined in particular by the generally accepted accounting principles or the generally accepted principles of computer-assisted accounting systems. Examples that can be mentioned here include:

- Documentation
- System configuration and access protection
- Data backup and recovery procedures
- Completeness and promptness of the archiving
- Immutability of the documents
- Long-term legibility and recoverability

The requirements that are defined in the context of this interpretation refer on the one hand directly to the IT systems that are used for accounting or retention purposes (e.g. reproducibility of the system, documentation of the system), but, on the other, also the environment in which such systems are operated (e.g. IT environment, IT organisation, internal control system). Here, how-ever, only a relatively abstract framework in which a permissible solution has to manoeuvre is defined, and no specific measures are prescribed. To a certain extent, requirements that are not covered by the IT system itself can thus be supported by organisational measures. On the other hand, organisational measures can be reduced if the IT systems in question themselves already cover the requirements.

## 1.6 Procedure and extent of the audit

KPMG conducted the audit in the period from 14 August 2014 to 19 December 2014 at the premises of the company in Schwäbisch Gmünd and also at the business premises of KPMG Frankfurt. The nature and extent of the audit procedures were recorded in our working papers.

All the information requested was readily issued to KPMG by the employees of GRAU DATA. The documents required were provided to KPMG. Findings and assessments concerning the facts are based on the test system set up at the time of the audit. The management confirmed in writing to KPMG that the statements and verifications issued, the process documentation provided and the product development measures are complete.

The procedure adopted to implement the software audit was conducted in accordance with the above-mentioned audit principles. Accordingly, the following audit areas were covered by reference to IDW PS 880:

**Review of and introduction to the subject of the audit**

At the beginning of the audit, a review was performed of the subject of the audit (application software) and of the test environment (hardware configuration, operating system components used and network configurations).

**Audit of the documentation**

The process documentation was audited in this auditing step. The process documentation consists of the system documentation and the user documentation. In the audit of the system documentation, it was assessed whether and how the technical components, processes and settings for the proper use of the software are presented in full and with sufficient clarity, transparency and comprehensibility.

The file transactions performed by GRAU DATA should satisfy the requirements of the GAAP and ensure in particular that the stored files are stored in unalterable form in accordance with the configuration chosen by the user and also cannot be removed from the data media.

**Audit of the programmed processing rules**

As part of the audit of the programmed processing rules, it was investigated whether the program sequences are correct, the programmed processing rules are objectively and logically correct and whether the plausibility checks contained in the program are effective.

The focus of this auditing step was the investigation of whether the legal requirements that necessarily have to be covered have been fulfilled. The audit of the processing functions was carried out by means of the test case method. Our procedure was directed at the basic functions of accounting-related software listed below, which we identified as key in the run-up to the audit:

- Configuration of the storage media to be used
- Storing of files
- Reading and changing of files
- Deletion of files

Existing test cases of GRAU DATA were used in our audit. It was a prerequisite that these were representative of the processing functions to be assessed. The test cases had to cover the basic functions described in the documentation and take into consideration the combination of functions representative of the work task. Furthermore, the test cases should also contain incorrect file transactions in order to audit whether permissible cases are correctly identified by the system and impermissible cases are rejected.

In addition, test cases prepared by KPMG were also used.

## 1.7 Disclosure of the software certification

Within the context of this engagement, the circumstances permitting the disclosure of the software certification to existing and potential FileLock users have been regulated. Subject to the regulation below, KPMG agrees to the disclosure of the report and/or of the software certification:

Posting on the Internet is subject to co-ordination with us concerning the specific design and to our express written approval.

GRAU DATA undertakes before disclosing the certification and/or the report concerning our work to a potential person with a justified interest to have this person sign a declaration of consent according to which the certificate and/or the report are to be handled in strict confi-

# 2 Audit results

## 2.1 Summary of the audit results

KPMG conducted an audit in accordance with auditing standard IDW PS 880 of the Institut der Wirtschaftsprüfer, "Audit of Software Products". This included the audit of the process documentation, the software development process and the software security as the basis of the program functions. In this process, access protection, parameter maintenance and the data backup and recovery procedure were taken into consideration as important aspects of the software security. Subsequently, the appropriateness and functionality of the necessary program functions and of the basic program functions were audited.

As a result of our **audit of the process documentation and of the software development processes**, we find that the correctness and completeness of the process documentation are clearly defined, and nothing gave rise to any objections. In the audit of the software development processes, it must be noted that changes are not always assigned to releases/versions and thus a subsequent assignment is not possible.

As a result of our **audit of the appropriateness and functionality of the program functions** and **of the software security**, we find that, when used properly, the audited version 2.3 of the FileLock archive solution enables electronic archiving within the meaning of IDW pronouncement FAIT 3 on the long-term and unalterable storage of accounting-related documents on machine-readable data media in fulfilment of the legal retention duties in accordance with Section 257 HGB and also ensures compliance with the Austrian and Swiss regulations. It is a prerequisite that the Enhanced Security Mode (ESM) is activated before the product goes live.

The security of the encryption method used within the framework of the Enhanced Security Mode (ESM) (see Section 3.3) was not the subject of the investigation. The key objective of ESM is to ensure that other applications, user and operating system functions cannot access protected data without using FileLock or by by-passing FileLock. We tested the function of this encryption, and this did not lead to any objections.

accepted principles for the proper keeping and retention of books, records and documents in electronic form and for data access) of 14 November 2014.

As software products are adapted to the requirements of the field of application, the opinion of KPMG can refer exclusively to the fact that the software product enables the criteria to be fulfilled when it is used properly.

We believe that the audit evidence we have obtained is sufficient and appropriate to provide a reasonable basis for our audit opinion.

In our opinion, based on the findings of our audit, version 2.3 of the FileLock software product audited by us enables archiving in compliance with the generally accepted accounting principles when it is used properly and satisfies the criteria listed above.

We issue this audit report on the basis of the contract entered into with GRAU DATA AG, the basis of which is formed by the attached General Engagement Terms for Auditors and Auditing Firms of 1 January 2002, also with effect for third parties, including the extended limitation of liability on the condition that the maximum indemnity limits contained therein apply jointly to all persons who receive this audit report with our prior consent. In addition to the maximum indemnity amount of EUR 4 million specified in no. 9 Section 2 clause 1 of the GET, we are liable to the amount of EUR 5 million specified in no. 9 Section 2 clause 5 of the GET in respect of damages caused by negligence. Broadening of liability shall not apply to damages for which a maximum indemnity is regulated by law.

Frankfurt am Main, 19 February 2015

*KPMG AG*
*Wirtschaftsprüfungsgesellschaft*

ppa.

Armin Weyell
*Partner*
*German Public Auditor*

Oliver Pfeiffer
*Senior Manager*

Within the context of the certification, functions that are relevant and key for the fulfilment of the requirements of commercial and tax law have been audited from all the FileLock components described in brief below. The focal points of the certification audit were derived from the requirements of IDW FAIT 3, which considers the requirements of the archiving regulations.

### 3.1.3 Description of the test environment used

The test environment provided to us consisted of the following components:

**VPN server:**

FileLock was provided on a server of GRAU DATA for the audit. All requirements concerning the operating system, the versioning and configurations are consistent with the documentation description and thus the original delivery. Therefore the audit was conducted in an environment that did not required any further adjustments and that was functional at the beginning of the audit:

| Components | Description / parameters |
|---|---|
| CPU | Intel Core i7 3520M |
| Main memory | 8.00 GB |
| Hard drive | 25 GB |
| Operating system | Windows Server 2008 R2 Standard |
| FileLock software | Version 2.3 |

### 3.1.4 Audit of the process documentation

A major prerequisite for the proper use of the software by the end user is the existence of appropriate process documentation. The necessary elements of process documentation are the system and user documentation, where the user documentation describes how to handle the software as well as the range of functions from a functional viewpoint, while the system documentation describes the same aspects from a technical system viewpoint.

In accordance with the requirements of IDW PS 880, KPMG organised the audit procedures in a targeted way in order to assess whether the process documentation is complete, reproducible and comprehensible. Furthermore, KPMG audited the factual accuracy of the user documentation to see whether the contents are consistent with the actual processing method of the software.

In principle, all software changes must go live as part of the version change, or versioning. A new FileLock version is being planned as a project organisation.

All changes must be adequately tested and approved before they are implemented, so that the changes can be incorporated in a new version package. However, changes are not always as-signed to releases/versions, so that it was not always possible to assign them subsequently during the audit. The central documentation tool for the administration of changes is Bugzilla. This tool records a ticket and assigns it a priority for each change. The processing status of the individual tickets is logged automatically and can be seen in the system. The product "Testlink" is used for logging and approving the test scenarios. Function tests that are conducted are archived and documented in a verifiable manner.

On the basis of sampling, KPMG audited the plausibility of the tickets in terms of their impacts on the propriety and the range of functions. Nothing gave rise to any objections in this process.

The software development process fulfils the requirements set within the audit.

Individual changes are tracked and processed in the development tool. Changes are compiled into new releases, which are tested using comprehensive test catalogues before they go live. The sale of a new version will require a successful test process.

It was not possible to present a dedicated change log showing which individual change has gone live in the past years specifically with which release.

We recommend in future that each individual change be assigned a release in the development tool use in order to increase the traceability.

## 3.3 Audit of the software security functions

### 3.3.1 Administration

The administration of the FileLock software is performed by the Windows operating system environment. After the software has been successfully installed on the storage system, hard drive partitions can be converted into the appropriate WORM volumes.

In order to ensure technical immutability, various products have become established on the hardware and software market that as WORM media (write once read many) are designed to ensure that once data and documents have been archived they can subsequently no longer be changed. To this end, the FileLock software deactivates all basic functions of the operating system in order to permanently prevent any deletions, overwrites and changes on a storage system and all documents it contains.

hanced Security Mode has been set up, all read and write access operations of the storage system are executed via this key.

**3) Selection of the DLR archiving function:** All documents within a partition or a folder are given the same archiving period when the DLR function is selected. One advantage here is that extensions of the retention period can be passed on comprehensively to all documents.

**4) Selection of the SFR archiving function:** The SFR function allows the administrator to configure individual retention periods for each individual document within a partition or folder. In this configuration, a minimum retention period, a default value and a maximum retention period are selected as indicators.

**5) Activation of the AutoCommit function:** Documents that are filed on a storage system operated by FileLock can be automatically archived by using the AutoCommit function. Alternatively, manually activating write protection can initiate archiving.

The configuration of the folder structure is carried out using Windows Explorer. User accounts and groups and access protection are also managed using the directory service of Microsoft Windows servers. Configurations of the folder structure, the user accounts and groups can no longer changed after the WORM volumes have been activated and to that effect have to be defined in advance. FileLock is set up in these areas on a Windows operating system environment and uses existing functions as interfaces. For this reason, knowledge of Windows administration is required. As a differentiation between access rights and compliance with separations of functions takes place exclusively through the operation system and FileLock does not offer any user administration options, audit procedures were set up to by-pass the access permissions and thus to amend documents.

As part of the audit, we installed the FileLock software as an administrator in the Windows operating system environment, set up storage systems accordingly and analysed and tracked impacts in the configurations of the folder structure, the user accounts and groups and the access protection. This did not lead to any objections.

### 3.3.2 Data backup and recovery procedure

In the replication, the same data was stored several times in different environments and synchronised automatically to the greatest extent possible. Replication serves to make data available at several locations. This helps to back up data on the one hand and, on the other, to reduce response times. Master/slave replication distinguishes between the original (primary) data and the dependent copies. During replication, there is a certain time span between the processing or creation of the primary data and its replication.

The replication service offered by FileLock – FileLock Replication Service – enables automatic synchronisation of the data of the FileLock volume with a defined target volume. This replication is a one-off, one-way replication from the source to the destination. Automatic reverse

an Federal Fiscal Code (BAO) and the Swiss Code of Obligations in conjunction with the Swiss Business Records Ordinance (GeBüV) as of 1 January 2013.

#### 3.4.1.1 Time stamp / time synchronisation

**Time stamp**

A time stamp is used in order to assign an event to an unambiguous time. A digital time stamp is applied in line with a defined format. It should be designed to be forgery-proof, as proof of times of events can be furnished with the time stamp. Digital time stamps are proof that an electronic document was submitted to the issuer of the time stamp at the time indicated.

Data that is stored in a directory secured by FileLock is given this time stamp after the document has been filed in the directory and a defined handover time has expired or as a result of the manual affixing of the time stamp. After the time stamp is affixed to the document, the retention period commences and the data is protected against all revisions.

**Verified Retention Clock (VRC)**

In order to ensure the retention period of the archiving system and thus the conformity with the rules, the FileLock product features an integrated verification method that guarantees that the time stamp cannot be changed, adapts interventions from external effects and calculates the retention period constantly in line with the defined value. External effects are understood to be modifications of the system clock, restarts or the shutdown of the system.

If modifications are carried out during the term, a compensation value is automatically generated which ensures that the data is not released for deletion in deviation from the retention period. Time differences resulting from the above-mentioned external effects can be logged for a maximum of one week per year.

As part of the audit of the time stamp, documents were filed in the storage system and the accuracy of the archiving stamp was audited. The audit procedures to ensure the accuracy of the VRC were manual system restarts and comparisons of the different controls and additionally system maintenance conducted by GRAU DATA. Our audits have not lead to any objections.

#### 3.4.1.4 Long-term legibility and recoverability

The purpose of archiving software is to guarantee the long-term legibility and recoverability of the archived data.

To this end, it must be ensured that all documents can continue to be retrieved and displayed during and after archiving. As FileLock builds on the functions of the Windows operating system, the ability to read and recover documents is guaranteed by the system. Furthermore, the long-term legibility and availability of the data depends on the life of the hard drives or storage systems used for FileLock.

Should the storage system be moved or the FileLock program deleted, FileLock and the encryption method must be reinstalled in order to regain access to the data and documents that continue to be archived. The protection against change thus remains in place, with the files protected against unauthorised access. If the licence key is lost, the test version can provide two weeks' access to the partitions.

As part of the audit, the legibility was verified during the retention period, after it had expired and the FileLock software was uninstalled. The legibility of the archived documents was always guaranteed during this process and the requirements set are thus fulfilled.

# Appendix
# General Engagement Terms

[Translator's notes are in square brackets]

# General Engagement Terms

for

## Wirtschaftsprüfer and Wirtschaftsprüfungsgesellschaften

[German Public Auditors and Public Audit Firms]

as of January 1, 2002

This is an English translation of the German text, which is the sole authoritative version

### 1. Scope

(1) These engagement terms are applicable to contracts between Wirtschaftsprüfer [German Public Auditors] or Wirtschaftsprüfungsgesellschaften [German Public Audit Firms] (hereinafter collectively referred to as the "Wirtschaftsprüfer") and their clients for audits, consulting and other engagements to the extent that something else has not been expressly agreed to in writing or is not compulsory due to legal requirements.

(2) If, in an individual case, as an exception contractual relations have also been established between the Wirtschaftsprüfer and persons other than the client, the provisions of No. 9 below also apply to such third parties.

### 2. Scope and performance of the engagement

(1) Subject of the Wirtschaftsprüfer's engagement is the performance of agreed services – not a particular economic result. The engagement is performed in accordance with the Grundsätze ordnungsmäßiger Berufsausübung [Standards of Proper Professional Conduct]. The Wirtschaftsprüfer is entitled to use qualified persons to conduct the engagement.

(2) The application of foreign law requires – except for financial attestation engagements – an express written agreement.

(3) The engagement does not extend – to the extent it is not directed thereto – to an examination of the issue of whether the requirements of tax law or special regulations, such as, for example, laws on price controls, laws limiting competition and Bewirtschaftungsrecht [laws controlling certain aspects of specific business operations] were observed; the same applies to the determination as to whether subsidies, allowances or other benefits may be claimed. The performance of an engagement encompasses auditing procedures aimed at the detection of the defalcation of books and records and other irregularities only if during the conduct of audits grounds therefor arise or if this has been expressly agreed to in writing.

(4) If the legal position changes subsequent to the issuance of the final professional statement, the Wirtschaftsprüfer is not obliged to inform the client of changes or any consequences resulting therefrom.

### 3. The client's duty to inform

(1) The client must ensure that the Wirtschaftsprüfer – even without his special request – is provided, on a timely basis, with all supporting documents and records required for and is informed of all events and circumstances which may be significant to the performance of the engagement. This also applies to those supporting documents and records, events and circumstances which first become known during the Wirtschaftsprüfer's work.

(2) Upon the Wirtschaftsprüfer's request, the client must confirm in a written statement drafted by the Wirtschaftsprüfer that the supporting documents and records and the information and explanations provided are complete.

### 4. Ensuring independence

The client guarantees to refrain from everything which may endanger the independence of the Wirtschaftsprüfer's staff. This particularly applies to offers of employment and offers to undertake engagements on one's own account.

### 5. Reporting and verbal information

If the Wirtschaftsprüfer is required to present the results of his work in writing, only that written presentation is authoritative. For audit engagements the long-form report should be submitted in writing to the extent that nothing else has been agreed to. Verbal statements and information provided by the Wirtschaftsprüfer's staff beyond the engagement agreed to are never binding.

### 6. Protection of the Wirtschaftsprüfer's intellectual property

The client guarantees that expert opinions, organizational charts, drafts, sketches, schedules and calculations – expecially quantity and cost computations – prepared by the Wirtschaftsprüfer within the scope of the engagement will be used only for his own purposes.

### 7. Transmission of the Wirtschaftsprüfer's professional statement

(1) The transmission of a Wirtschaftsprüfer's professional statements (long-form reports, expert opinions and the like) to a third party requires the Wirtschaftsprüfer's written consent to the extent that the permission to transmit to a certain third party does not result from the engagement terms.

The Wirtschaftsprüfer is liable (within the limits of No. 9) towards third parties only if the prerequisites of the first sentence are given.

(2) The use of the Wirtschaftsprüfer's professional statements for promotional purposes is not permitted; an infringement entitles the Wirtschaftsprüfer to immediately cancel all engagements not yet conducted for the client.

### 8. Correction of deficiencies

(1) Where there are deficiencies, the client is entitled to subsequent fulfillment [of the contract]. The client may demand a reduction in fees or the cancellation of the contract only for the failure to subsequently fulfill [the contract]; if the engagement was awarded by a person carrying on a commercial business as part of that commercial business, a government-owned legal person under public law or a special government-owned fund under public law, the client may demand the cancellation of the contract only if the services rendered are of no interest to him due to the failure to subsequently fulfill [the contract]. No. 9 applies to the extent that claims for damages exist beyond this.

(2) The client must assert his claim for the correction of deficiencies in writing without delay. Claims pursuant to the first paragraph not arising from an intentional tort cease to be enforceable one year after the commencement of the statutory time limit for enforcement.

(3) Obvious deficiencies, such as typing and arithmetical errors and formelle Mängel [deficiencies associated with technicalities] contained in a Wirtschaftsprüfer's professional statements (long-form reports, expert opinions and the like) may be corrected – and also be applicable versus third parties – by the Wirtschaftsprüfer at any time. Errors which may call into question the conclusions contained in the Wirtschaftsprüfer's professional statements entitle the Wirtschaftsprüfer to withdraw – also versus third parties – such statements. In the cases noted the Wirtschaftsprüfer should first hear the client, if possible.

### 9. Liability

*(1) The liability limitation of § ["Article"] 323 (2)["paragraph 2"] HGB ["Handelsgesetzbuch": German Commercial Code] applies to statutory audits required by law.*

*(2) Liability for negligence; An individual case of damages*

If neither No. 1 is applicable nor a regulation exists in an individual case, pursuant to § 54a (1) no. 2 WPO ["Wirtschaftsprüferordnung": Law regulating the Profession of Wirtschaftsprüfer] the liability of the Wirtschaftsprüfer for claims of compensatory damages of any kind – except for damages resulting from injury to life, body or health – for an individual case of damages resulting from negligence is limited to € 4 million; this also applies if liability to a person other than the client should be established. An individual case of damages also exists in relation to a uniform damage arising from a number of breaches of duty. The individual case of damages encompasses all consequences from a breach of duty without taking into account whether the damages occurred in one year or in a number of successive years. In this case multiple acts or omissions of acts based on a similar source of error or on a source of error of an equivalent nature are deemed to be a uniform breach of duty if the matters in question are legally or economically connected to one another. In this event the claim against the Wirtschaftsprüfer is limited to € 5 million. The limitation to the fivefold of the minimum amount insured does not apply to compulsory audits required by law.

*(3) Preclusive deadlines*

A compensatory damages claim may only be lodged within a preclusive deadline of one year of the rightful claimant having become aware of the damage and of the event giving rise to the claim – at the very latest, however, within 5 years subsequent to the event giving rise to the claim. The claim expires if legal action is not taken within a six month deadline subsequent to the written refusal of acceptance of the indemnity and the client was informed of this consequence.

The right to assert the bar of the preclusive deadline remains unaffected. Sentences 1 to 3 also apply to legally required audits with statutory liability limits.



52002 KND
1/2002

10. Supplementary provisions for audit engagements

(1) A subsequent amendment or abridgernent of the financial statements or management report audited by a Wirtschaftsprüfer and accompanied by an auditor's report requires the written consent of the Wirtschaftsprüfer even if these documents are not published. If the Wirtschaftsprüfer has not issued an auditor's report, a reference to the audit conducted by the Wirtschaftsprüfer in the management report or elsewhere specified for the general public is permitted only with the Wirtschaftsprüfer's written consent and using the wording authorized by him.

(2) If the Wirtschaftsprüfer revokes the auditor's report, it may no longer be used. If the client has already made use of the auditor's report, he must announce its revocation upon the Wirtschaftsprüfer's request.

(3) The client has a right to 5 copies of the long-form report. Additional copies will be charged for separately.

11. Supplementary provisions for assistance with tax matters

(1) When advising on an individual tax issue as well as when furnishing continuous tax advice, the Wirtschaftsprüfer is entitled to assume that the facts provided by the client – especially numerical disclosures – are correct and complete; this also applies to bookkeeping engagements. Nevertheless, he is obliged to inform the client of any errors he has discovered.

(2) The tax consulting engagement does not encompass procedures required to meet deadlines, unless the Wirtschaftsprüfer has explicitly accepted the engagement for this. In this event the client must provide the Wirtschafts-prüfer, on a timely basis, all supporting documents and records – especially tax assessments – material to meeting the deadlines, so that the Wirtschafts-prüfer has an appropriate time period available to work therewith.

(3) In the absence of other written agreements, continuous tax advice encompasses the following work during the contract period:

a) preparation of annual tax returns for income tax, corporation tax and business tax, as well as net worth tax returns on the basis of the annual financial statements and other schedules and evidence required for tax purposes to be submitted by the client

b) examination of tax assessments in relation to the taxes mentioned in (a)

c) negotiations with tax authorities in connection with the returns and assessments mentioned in (a) and (b)

d) participation in tax audits and evaluation of the results of tax audits with respect to the taxes mentioned in (a)

e) participation in Einspruchs- und Beschwerdeverfahren [appeals and complaint procedures] with respect to the taxes mentioned in (a).

In the afore-mentioned work the Wirtschaftsprüfer takes material published legal decisions and administrative interpretations into account.

(4) If the Wirtschaftsprüfer receives a fixed fee for continuous tax advice, in the absence of other written agreements the work mentioned under paragraph 3 (d) and (e) will be charged separately.

(5) Services with respect to special individual issues for income tax, corporate tax, business tax, valuation procedures for property and net worth taxation, and net worth tax as well as all issues in relation to sales tax, wages tax, other taxes and dues require a special engagement. This also applies to:

a) the treatment of nonrecurring tax matters, e. g. in the field of estate tax, capital transactions tax, real estate acquisition tax

b) participation and representation in proceedings before tax and administrative courts and in criminal proceedings with respect to taxes, and

c) the granting of advice and work with respect to expert opinions in connection with conversions of legal form, mergers, capital increases and reductions, financial reorganizations, admission and retirement of partners or shareholders, sale of a business, liquidations and the like.

(6) To the extent that the annual sales tax return is accepted as additional work, this does not include the review of any special accounting prerequisities nor of the issue as to whether all potential legal sales tax reductions have been claimed. No guarantee is assumed for the completeness of the supporting documents and records to validate the deduction of the input tax credit.

12. Confidentiality towards third parties and data security

(1 ) Pursuant to the law the Wirtschaftsprüfer is obliged to treat all facts that he comes to know in connection with his work as confidential, irrespective of whether these concern the client himself or his business associations, unless the client releases him from this obligation.

(2) The Wirtschaftsprüfer may only release long-form reports, expert opinions and other written statements on the results of his work to third parties with the consent of his client.

(3) The Wirtschaftsprüfer is entitled – within the purposes stipulated by the client – to process personal data entrusted to him or allow them to be processed by third parties.

13. Default of acceptance and lack of cooperation on the part of the client

If the client defaults in accepting the services offered by the Wirtschaftsprüfer or if the client does not provide the assistance incumbent on him pursuant to No. 3 or otherwise, the Wirtschaftsprüfer is entitled to cancel the contract immediately. The Wirtschaftsprüfer's right to compensation for additional expenses as well as for damages caused by the default or the lack of assistance is not affected, even if the Wirtschaftsprüfer does not exercise his right to cancel.

14. Remuneration

(1 ) In addition to his claims for fees or remuneration, the Wirtschaftsprüfer is entitled to reimbursement of his outlays: sales tax will be billed separately. He may claim appropriate advances for remuneration and reimbursement of outlays and make the rendering of his services dependent upon the complete satisfaction of his claims. Multiple clients awarding engagements are jointly and severally liable.

(2) Any set off against the Wirtschaftsprüfer's claims for remuneration and reimbursement of outlays is permitted only for undisputed claims or claims determined to be legally valid.

15. Retention and return of supporting documentation and records

(1) The Wirtschaftsprüfer retains, for ten years, the supporting documents and records in connection with the completion of the engagement – that had been provided to him and that he has prepared himself – as well as the correspondence with respect to the engagement.

(2) After the settlement of his claims arising from the engagement, the Wirtschaftsprüfer, upon the request of the client, must return all supporting documents and records obtained from him or for him by reason of his work on the engagement. This does not, however, apply to correspondence exchanged between the Wirtschaftsprüfer and his client and to any documents of which the client already has the original or a copy. The Wirtschaftsprüfer may prepare and retain copies or photocopies of supporting documents and records which he returns to the client.

16. Applicable law

Only German law applies to the engagement, its conduct and any claims arising therefrom.