Report and Software Certification on the Audit of the Archiving Software FileLock Version 2.4

GRAU DATA GmbH
Schwäbisch Gmünd

rdxLock Version 2.4

OEM partner Overland-Tandberg

Table of contents

List of abbreviations

AO	Abgabenordnung [German Fiscal Code]
CFTC	Commodity Futures Trading Commission
CPU	Central Processing Unit
DLR	Directory Level Retention
DV	Datenverarbeitung [Data processing]
ESM	Enhanced Security Mode
FAIT	Fachausschuss für Informationstechnologie [Technical Committee for Information Technology]
GB	Gigabyte
GET	Allgemeine Auftragsbedingungen [General Engagement Terms]
GoB	Grundsätze ordnungsmäßiger Buchführung [Generally accepted accounting principles (GAAP)]
GoBD	Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff [Generally accepted principles for the proper keeping and retention of books, records and documents in electronic form and for data access]
GPT	Globally Unique Identifier Partition Table
GUI	Graphical User Interface
HGB	Handelsgesetzbuch [German Commercial Code]
IAS	International Accounting Standards
IDW	Institut der Wirtschaftsprüfer [Institute of Public Auditors in Germany]
IFRS	International Financial Reporting Standards
MBR	Master Boot Record
NTFS	New Technology File System
OEM	Original Equipment Manufacturer
PS	Prüfungsstandard – Auditing Standards
RO	Read Only
SEC	Securities and Exchange Commission
SFR	Single File Retention
VO	Verordnung – Regulation
WORM	Write Once Read Many

1 Contents and performance of the engagement

1.1 Audit engagement

The management of

GRAU DATA GmbH, 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 12 October 2017 to audit the compliance of version 2.4 of the FileLock standard archiving software with the requirements of SEC 17a/4F of the US Securities and Exchange Commission and the CFTC 1.31 (b) – (c) requirements of the Commodity Futures Trading Commission.

FileLock is already certified in the version 2.3 according to the IDW PS 880 auditing standard of the German Institute of Auditors, "Audit of Software Products" by KPMG in 2014. Our audit procedures throughout this audit confirms that no significant changes have been made to the software since 2014.

On account of the functions of the software, the assessment was carried out essentially on the requirements of the US Securities and Exchange Commission SEC 17a/4F and the Commodity Futures Trading Commission CFTC 1.31 (b) – (c). SEC Rule 17a/4F is a regulation issued by the U.S. Securities and Exchange Commission pursuant to its regulatory authority under the US Securities Exchange Act of 1934 (Known simply as the "Exchange Act") which outlines requirements for electronic storage media to maintain records required to be retained. The requirements defines the retention, indexing and accessibility of accounting related documents subject for companies. The Commodity Futures Trading Commission CFTC 1.31 (b) – (c) also demands these requirements.

SEC Rule 17a/4F and CFTC 1.31 (b) – (c) specifies compliance requirements for the storage and operation of archived records in electronic form. Under these rules, electronic records must be preserved exclusively in a non-rewriteable and non-erasable format. The archive system must therefore prevent the records from being changed or deleted during the prescribed retention period.

The above mentioned rules are guiding principles. Due to the lack of detail of the SEC and CFTC requirements and the overlap of all requirements with the German IDW Accounting Practice Statement, the engagement was also carried out 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 that enables archiving of data in unalterable form on existing disk storage systems. This Windows based software solution provides audit-proof archiving (WORM – Write Once Read Many) where data cannot be deleted or overwritten. FileLock is also sold by the OEM partner Overland-Tandberg under their own brand name "rdxLock". rdxLock Version 2.4 is also covered by this report and certificate. FileLock 2.4/rdxLock 2.4 differs from the previous version FileLock/rdxLock 2.3.2 only in the limitation of the permissible operating systems. There were no further changes and adaptations to the software made – based on our audit -, so that this report and certificate also covers FileLock version 2.3.2 and rdxLock 2.3.2 (see chapter 3.2).

The subject matter of the service performed by KPMG was the audit of the FileLock software in the version 2.4 in terms of the unalterable storage of data on various storage media in accordance with the regulatory requirements of the US Securities and Exchange Commission SEC 17a/4F and the Commodity Futures Trading Commission CFTC 1.31 (b) – (c). The audit is also performed on the basis of IDW RS FAIT 3 because this standard contains more precise definitions for the SEC and CFTC requirements for an archiving system. Accordingly, the objective of the software audit was to assess also 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.

The certification does not extend to subsequent versions of the software or to risks that result from a change in the legal framework after the audit was completed. The subject matter of the engagement did not include reviewing whether the data (e.g. log files) generated by the software was correct and appropriate.

Furthermore, the quality or security of the encryption technique used was not the subject matter of the audit.

It is pointed out that the assessment of to what extent the services performed by KMPG are adequate and appropriate for your purposes is your sole responsibility.

All system based audit procedures were performed by using a test system provided by GRAU DATA and test data created for the audit. Business transactions that usually arise in a company were selected as test cases.

The audit was not conducted in an actual company environment, which means that it was not possible to take into account the designed operating effectiveness of the internal control system (ICS) inherent at a company.

1.2 Auditing Standards

The following auditing standards and legal requirements as well as application-specific test criteria formed the basis of our audit:

- Regulatory requirements of the US Securities and Exchange Commission SEC 17a/4F;
- Commodity Futures Trading Commission CFTC 1.31 (b) – (c);
- IDW Auditing Standards "Audit of Software Products" (IDW PS 880) as amended on 11 March 2010
- Regulations of German commercial and tax law (Sections 238, 239 and 257 HGB and Sections 145, 146 and 147 AO);
- Regulations of Austrian and Swiss commercial and tax law, including Section 132 of the Austrian Federal Fiscal Code (BAO) and the Swiss Code of Obligations in conjunction with the Swiss Business Records Ordinance (GeBüV) as of 1 January 2013;
- The German "Grundsätze ordnungsmäßiger Buchführung" (GoB – Generally accepted accounting principles (GAAP));
- IDW Accounting Practice Statement "Principles of Proper Accounting when using Information Technology" as amended on 24 September 2002 (IDW RS FAIT 1);
- IDW Accounting Practice Statement "Principles of Proper Accounting when using Electronic Archiving Procedures" (IDW RS FAIT 3) of 11 July 2006;
- "Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff" (GoBD – Generally accepted principles for the proper keeping and retention of books, records and documents in electronic form and for data access) of 14 November 2014.

1.3 Engagement terms

Our offer is based on the "General Engagement Terms" (Allgemeine Auftragsbedingungen für Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften) as of January 1, 2017. In extension of the liability limitation sum specified in Sec. 9 (2) of the General Terms the maximum amount of liability of EUR 4m for damages resulting from negligence will be limited to EUR 5m. The amount specified in Sec. 9 (5) of the General Terms of EUR 5m will remain unaffected. Extensions of liability limitations shall not apply to damages for which liability limitation sums are stipulated 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 requirements of the US Securities and Exchange Commission SEC 17a/4F and the Commodity Futures Trading Commission CFTC 1.31 (b) – (c) as well as GAAP form the basis for the assessment of whether FileLock is in conformity with these regulations.

In addition to the regulatory requirements of the US Securities and Exchange Commission SEC 17a/4F and the Commodity Futures Trading Commission CFTC 1.31 (b) - (c) from the regulations and interpretations of the Handelsgesetzbuch (HGB) and the Abgabenordnung (AO) in Germany as well as the Swiss Code of Obligations (GeBüV) and the Austrian Federal Legislation (BAO) and stipulate verifiable compliance with the requirements of an internal control system (ICS), which are defined in particular by the generally accepted accounting principles or the generally accepted principles of computer-aided accounting systems.

The following requirements of the US Securities and Exchange Commission SEC 17a/4F and the Commodity Futures Trading Commission CFTC 1.31 (b) - (c) are placed on the archiving system: Determination of the duration of the storage of data and documents in the IT-supported Accounting system as well as the definition of retention periods for data and documents to be archived electronically. An appropriate indexation procedure and the ability to unequivocally allocate archived documents and data for accounting purposes. Procedures and techniques for verifiably complete and correct collection, archiving, deletion and readability of archived documents and data Method for accessing documents and data in stored archive databases. Ensure immutability, so that technical and organizational measures are taken to ensure that no subsequent changes are made to electronically archived documents and data. The stored documents and data must be reproducible at any time during the entire retention period. The documents and data can be made readable via the online display of the documents and data, by creating a printout or by providing the documents and data in a format that can be evaluated automatically via an export interface of the archiving system.

In summary, the following requirements for an archive system must be fulfilled:

- 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

On the basis of these requirements, an assessment was subsequently made to determine to what extent FileLock provides functions that fulfil the requirements or can at least support fulfilment of the requirements and whether compensating measures are necessary.

The result is a statement on to what extent the product investigated supports the fulfilment of the requirements for conformity with the regulations.

1.5 Requirements of commercial and tax law

German, Austrian and Swiss commercial and tax law as well as the requirements of the US Securities and Exchange Commission SEC 17a/4F and the Commodity Futures Trading Commission CFTC 1.31 (b) – (c) defines extensive requirements that affect almost every company in Germany, Austria and Switzerland. Although the perspective of German commercial law (here the Commercial Code – HGB) and tax law (here essentially the Fiscal Code – AO) and of the Swiss Code of Obligations (here the Business Records Ordinance – GeBüV) and the regulatory requirements of the US Securities and Exchange Commission SEC 17a/4F and the Commodity Futures Trading Commission CFTC 1.31 (b) – (c) differs, accounting and recording duties are defined on all sides as a key aid for achieving these goals. In addition to these regulations, there is a large number of other requirements which may be relevant for companies in Germany, Austria and Switzerland, but which have not been considered here. They may have the characteristics of civil or criminal law (e.g. Civil Code, Criminal Code), relate to legal form (e.g. Companies Act, Act on limited liability companies) or be specific to a sector (e.g. Banking Act, Insurance Supervision Act), or they may also stem from foreign countries (e.g. Sarbanes-Oxley Act – SOX, Electronic Discovery Act). The requirements governing the formal structure of accounts and retention are not exhaustively regulated in detail in German, Austrian and Swiss commercial and tax law.

The requirements regulates only isolated circumstances specifically, such as:

- Comprehensibility of the accounting (explanation of abbreviations, figures, letters or symbols used);
- The language used (use of a modern language, a translation can be required if a language other than German is used);
- Place of the accounting (principle: domestic, exceptions are possible).

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, however, 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 relevant IT systems already cover the requirements on their own.

1.6 Procedure and extent of the audit

KPMG conducted the audit in the period from 23 October 2017 to 10 November 2017 at the premises of the company in Schwäbisch Gmünd and also at the 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 SEC 17a/4F, CFTC 1.31 (b) – (c), IDW PS 880 and HGB.

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 (operating system components used that affect the functionality of Filelock).

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 user documentation was assessed in terms of the minimum requirements pursuant to SEC 17a/4F, CFTC 1.31 (b) – (c), IDW PS 880 and HGB (whether there is user documentation and whether it is complete, free of errors, clear and accessible).

In addition to the process documentation, it was audited whether the organisational measures and agreements provided for are suitable for creating an understanding of the documentation process within a reasonable time for an expert third party.

Assessment of the program development, maintenance and approval

In order to assess the possibilities for future maintenance of the program, the technical IT tools and the organisational measures used during the program development were investigated. The approval process and the maintenance methods for the program were also assessed.

Audit of the software security

a) Audit of the segregation of access rights

The purpose of the differentiation of access authorizations was to determine whether the software supports compliance with the principal of minimal rights and considers the segregation of duties. Specifically, it was examined whether and to what extent the software - in interaction with the operating system or a superordinate security system - allows it, by assigning user IDs and passwords as well as assigning authorizations. For this purpose, configuration options with administrative rights were tested and the system's response to access tabs in read and write access was checked. Within the scope of the audit, we tested those operating system components that affect the functionality of FileLock.

b) Audit of the data backup and recovery procedures

In the audit of the data backup and recovery procedures, the options provided by the software that enable data and programs to be back up periodically were assessed in connection with the system environment deployed.

Furthermore, it was investigated to what extent an orderly recovery of the system is possible after a system error and whether in the restored system environment the previously managed files can continue to be used as defined by the program.

Audit of the necessary processing functions

As part of the process audit, the processing functions that are of importance for compliance with the generally accepted accounting principles in software functionality of this kind were assessed. This includes in particular the tamper-proof archiving of files on various storage 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 during 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 contained also 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 coordination 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 confidence and we are subject to only limited liability in accordance with our General Engagement Terms. GRAU DATA indemnifies KPMG against all claims for damages and costs that are incurred as a result of a breach of this disclosure restriction.

GRAU DATA indemnifies KPMG against all claims for damages and costs that are incurred as a result of a breach of these regulations when the report and/or the software certification is disclosed.

The terms governing our engagement are set out in the General Engagement Terms [GET] for Auditors and Auditing Firms as amended on 1 January 2017 and attached in the appendix (see 1.3 Engagement Terms) including a specific liability extension agreement.

2 Audit results

2.1 Summary of the audit results

KPMG conducted an audit in accordance with the requirements of SEC 17a/4F of the US Securities and Exchange Commission and CFTC 1.31 (b) – (c) of the Commodity Futures Trading Commission and the 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. During the audit we can assign all changes to releases/versions. It must be noted, that for the customer only changes that affect the visible functionality of the software with regard to the graphical user interface are described in detail in corresponding release notes but changes which affects only the internal functionality of the software are not described in detail in the release notes for the customer.

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 2.4 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 and the regulatory requirements of the US Securities and Exchange Commission SEC 17a/4F and the Commodity Futures Trading Commission CFTC 1.31 (b) – (c). It is a prerequisite that enable worm mode is selected. Enhanced Security Mode (ESM) has to be "activated" in Version 2.4. This ensures that the volume resides on a primary partition of a disk with Master Boot Record (MBR) or Globally Unique Identifier Partition Table (GPT) partitioning schema. The end of the retention period is always represented in the last-access timestamp for the file object for SFR and DLR mode since version 2.3.1.

An encryption procedure is implemented. 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.

2.2 Software Certification

To the legal representatives of GRAU DATA GmbH.

GRAU DATA GmbH, Schwäbisch Gmünd, engaged KPMG on 12 October 2017 to perform an audit of the archiving product FileLock, version 2.4.

The legal representatives of the company are responsible for the software product and for the planning, implementation and monitoring of the software development. This responsibility is not affected by the audit by KPMG. Our responsibility was to express an opinion on version 2.4 of this software product based on the audit performed.

KPMG conducted its audit in accordance with the requirements requirements of SEC 17a/4F of the US Securities and Exchange Commission and CFTC 1.31 (b) – (c) of the Commodity Futures Trading Commission and also implies the standard "Audit of Software Products" of the Institut der Wirtschaftsprüfer (IDW PS 880) as amended on 11 March 2010. This standard requires that the software audit be planned and performed in such a way that it can assessed with reasonable assurance whether the software product allows accounting that complies with the generally accepted accounting principles when it is used properly and satisfies the criteria taken as the basis in accordance with the engagement.

This includes the assessment on the one hand of whether the criteria are appropriately implemented by the processing functions and by the internal control system and, on the other, of whether informative process documentation is available. The effectiveness of the program functions is assessed by means of test cases.

Reviewing whether the data (e.g. log files) generated by the software is correct and appropriate did not form part of the subject matter of the engagement.

In accordance with the engagement, the following criteria formed the basis of the audit:

- Regulatory requirements of the US Securities and Exchange Commission SEC 17a/4F;
- Commodity Futures Trading Commission CFTC 1.31 (b) – (c);
- Regulations of German commercial and tax law (Sections 238, 239 and 257 HGB and Sec-tions 145, 146 and 147 AO);
- Regulations of Austrian and Swiss commercial and tax law, including Section 132 of the Austrian Bundesabgabenordnung (BAO – Federal Fiscal Code) and Swiss Obligationenrecht (Code of Obligations) in conjunction with the Geschäftsbücherverordnung (GeBüV – Business Records Ordinance) as of 1 January 2013;
- The German "Grundsätze ordnungsmäßiger Buchführung" (GoB – Generally accepted accounting principles (GAAP));
- IDW Accounting Practice Statement "Principles of Proper Accounting when using Information Technology" as amended on 24 September 2002 (IDW RS FAIT 1);
- IDW Accounting Practice Statement "Principles of Proper Accounting when using Electronic Archiving Procedures" (IDW RS FAIT 3) of 11 July 2006;

- "Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff" (GoBD – Generally 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, Filelock version 2.4 / rdxlock version 2.4 / Filelock version 2.3.2 and rdxlock version 2.3.2 software products audited by us enables archiving in compliance with the above mentioned generally accepted accounting principles and criterias when it is used properly.

We issue this audit report on the basis of the contract entered into with GRAU DATA GmbH, the basis of which is formed by the attached General Engagement Terms for Auditors and Auditing Firms of 1 January 2017, 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, 22 December 2017

KPMG AG

Wirtschaftsprüfungsgesellschaft

ppa.

Armin Weyell	Oliver Pfeiffer
Partner	*Senior Manager*
German Public Auditor	

3 Performance of the audit and results in detail

3.1 Review and introduction to the software product

3.1.1 General

GRAU DATA is the manufacturer of the software called FileLock. The release-specific, hardware-independent FileLock standard software supports the archiving process by protecting accounting-related documents for a defined retention period from being deleted, changed, renamed and moved. In order to satisfy the legal requirements, accounting-related data can be deleted, but not changed, after the retention period has expired. Individual configuration options (e.g. archiving period, language setting to English) allow the software to be used in international corporations. Hardware independence and simplicity allow the client to install the product in existing IT infrastructure and an existing storage system. The integration of the product in existing storage systems is supported exclusively in Windows architectures. To this end, the FileLock program can be used to set up WORM-protected storage in which documents subject to retention requirements are stored and thus archived in a tamper-proof way. Regular release updates mean that users of the product can benefit from new developments.

Requirements of commercial and tax law are placed on technical archiving software applications in order to ensure that the processing is appropriately complete and factually correct and thus that generally accepted accounting principles are complied with.

3.1.2 Range of functions

The individual components of FileLock are integrated elements of the products. The product can be used exclusively for compliance with the retention requirements. Functions that enable indexing, administer signature verification keys or provide verification methods are not supported by FileLock, but can be implemented additionally by the customer's own archiving systems or archiving systems of third-party providers.

Components of FileLock

- Electronic archiving (WORM)
- Encryption process
- Time stamp / Verified Retention Clock
- FileLock Replication Service

Within the context of the certification, functions that are relevant and key for the fulfilment of the requirements 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 detailed requirements of the archiving regulations and covers all requirements defined in SEC 17a/4F and CFTC 1.31 (b) – (c).

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 require 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 2012 R2 Standard
FileLock software	Version 2.4

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, SEC 17a/4F and CFTC 1.31 (b) – (c) 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.

The process documentation consists of a product description and an administration, user, editor and operating manual. It has to describe the procedures used correctly and must be comprehensible to an expert third party. The process documentation has to be updated on a regular basis and is subject to the same retention requirements as the documents subject to accounting procedures that are recorded, created or processed by the processes described.

The user manual contains all information on the correct operation of the archive solution. The user documentation illustrates all the functions of the software in a user-friendly way for the end user and corresponds in its actuality to version 2.4.

The product description as well as the administration, editor and operating manual provide the technical system documentation and are directed at system administrators. In this documentation, the administration functions and settings for parametrisation and for configuring the interfaces are described.

We recommend to include release notes for major changes not only for the internal documentation but also for the customer.

Comparable requirements are also defined in German, Austrian and Swiss law.

KPMG considers the process documentation presented as suitable for ensuring proper use of the software by the end user and the system administrator.

3.2 Version and brand names of the software

FileLock was certified in version 2.3 in 2014. Based on the following audit procedure we analysed the changes in FileLock version 2.4. versus the version 2.3.2 and 2.3:

- As a part of the Audit, we have determined, that in version 2.3.2 compared to version 2.3 only customizing changes have been made which have no influence on the program logic
- The only difference between version 2.4 and version 2.3.2 is the limitation of the permitted operating systems in version 2.4, so that the installation of FileLock 2.4 on older operating systems is no longer possible. No further program changes have been made

Furthermore we audited the version 2.4. of FileLock with regard to the to SEC 17a/4F, CFTC 1.31 (b) – (c) and IDW PS 880 requirements.

The software FileLock is also sold by Tandberg as “rdxLock”, with similar version numbers.

Based on audit procedures we analysed to re-branding process to evaluate the changes to software during this process steps. The audit procedures showed that the software version of FileLock 2.4 and rdxLock 2.4. are the same besides the branding information. This is also the case for the software version 2.3.2 of both products.

3.3 Assessment of the software development procedure

The quality of the software development procedure has a direct influence on the proper implementation of the software functions as well as on the correctness and reliability of the development procedure of the software manufacturer. In this connection, the technical IT tools and the organisational measures employed in the development of the program are key for guaranteeing the future maintenance of the program. In particular, it should be possible here to furnish proof of the necessary version management and to create change documentation concerning the development environment and the library management programs.

The development (including debugging and further development) and the quality assurance of the software product are carried out by employees of GRAU DATA.

Changes to and further developments of the FileLock product must be performed at GRAU DATA in accordance with defined processes that are laid down in writing.

The development process and the software changes are based on the specifications of the Information Technology Infrastructure Library (ITIL). Changes to the program result from the incident management and from the change management at GRAU DATA.

Incident management involves the receipt and processing of errors that are reported, while change management basically involves requests to change to the product functions 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. The changes were in all cases no significant changes, which did not lead to any change in the functionality of FileLock. 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 for a release in the development tool used in order to increase the traceability.

3.4 Audit of the software security functions

3.4.1 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. Nevertheless, the activation of ESM is prerequisite to ensure the immutability of the data and documents (further details see below). 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.

It should be noted that the partition of the storage device must be configured as NTFS file format. Furthermore, local administrator privileges are a prerequisite for the successful configuration of the environment. The administrator has six setting options during the initial configuration.

In principle, FileLock enables main directories or sub-directories to be protected. In addition, it can be decided for each main and sub-directory whether Directory Level Retention (DLR) or Single File Retention (SFR) is chosen for the respective directory. Furthermore, Enhanced Security Mode (ESM) and the AutoCommit function are also available as further settings for the above-mentioned options:

1) Assigning of the archiving rules: The FileLock product offers two functions during the initial configuration of a data storage medium that define the archiving rules.

The first function allows the parameters of the retention period to be set up for the whole partition. Thus all documents on this partition are configured for one instance. In this option, a one-time choice must be made between Directory Level Retention (DLR) and Single File Retention (SFR).

The second function allows different parameters concerning the retention period to be assigned to individual folders within a partition. Furthermore, individual folders can be declared as DLR or SFR.

2) Activation of Enhanced Security Mode (ESM): ESM designates the encryption options. When ESM is activated, the protected data is encrypted and provides expanded protection against external effects**.** By activating this function, the immutability of the documents is ensured. If the encryption variants are not activated, all documents on the data storage medium can be modified by another computer. When this function is activated, the documents cannot be accessed without the FileLock software.

During encryption, the FileLock product chooses an encryption process that has been independently developed by GRAU DATA. The function prevents unauthorised parties accessing the protected partitions and supports the security aspect in the following scenarios:

- The FileLock application is deactivated on the storage system
- FileLock is uninstalled from the storage system
- The hard drive is connected to a server on which the FileLock software has not been installed.

Encryption is carried out by creating a device driver that reserves data blocks within the hard drive for use by FileLock. The data blocks are protected against unauthorised access. A random key is generated when a WORM volume is initialised. This key is in turn coded with a fixed key and stored in a data block. As a result, the entire area used by the file system on the volume is coded and encrypted, as are all data blocks in the data storage device. After Enhanced 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 archiving can be initiated by Snaplock or manually.

The configuration of the folder structure is carried out by 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 prohibits all activities to change data, independent from access permissions or administrator rights.

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.

3.4.2 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 replication does not take place. FileLock must also be installed on the target system and the storage systems must be configured identically in order to enable the primary data to be replicated. The logging by the Windows USN Journal is used to carry out the replication. This journal logs all file changes on data storage media and thus fulfils the criteria of the archiving process. Using this logging enables FileLock to carry out real-time replication. Furthermore, all metadata of the original document is taken over as a result of the identical configuration of the two volumes.

The replication method must be activated before the volumes are set up. If this is not complied with, manual steps have to be initiated in order to synchronise the target paths. The next steps are described in the administration manual.

As part of our audit, we administered the replication service and tracked the effects of the logging as well as the transfer values. The logging was always verifiable and complete and as result did not lead to any objections.

3.5 Audit of the appropriateness and functionality of the program functions

3.5.1 Archiving

Electronic archiving has to be distinguished from simple filing as temporary storage of documents, which can also be changed. In addition to the long-term character of archiving, immutability is an essential element of the archiving concept. The immutability of a document is the requirement that changes to the structure or contents are not permitted. The requirement for immutability mainly involves a consideration of the following requirements:

- Traceability of document-based procedures from creation to filing
- Completeness of the filed documents, completeness of one document (e.g. file size) and completeness of all filed documents (number of documents)
- Correctness of the filed data
- Authenticity as a requirement for unambiguous identification and incontestability, e.g. of the author of a document.

The essential functional requirements for electronic archiving can be found in pronouncements of the Institut der Wirtschaftsprüfer in Deutschland e.V. (IDW), such as the pronouncement of the Technical Committee for Information Technology (FAIT) "Grundsätze ordnungsmäßiger Buchführung beim

Einsatz elektronischer Archivierungsverfahren" (Principles of Proper Accounting when Using Electronic Archiving Procedures) (IDW RS FAIT 3) for example, as well as in the regulations of Austrian and Swiss commercial and tax law, including Section 132 of the Austrian Federal Fiscal Code (BAO) and the Swiss Code of Obligations in conjunction with the Swiss Business Records Ordinance (GeBüV) as of 1 January 2013. In addition SEC 17a/4F of the US Securities and Exchange Commission and CFTC 1.31 (b) – (c) of the Commodity Futures Trading Commission includes essential requirements.

3.5.1.1 Time stamp / Verified Retention Clock

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 are compensated 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. Furthermore, the server time has been changed to check if the retention period can be manipulated. Our audits have not lead to any objections.

3.5.1.2 Completeness of the archiving

A key requirement for archiving software such as FileLock is the complete and correct archiving of the data filed on the archiving device.

Depending on the configuration of the underlying directory, data filed in the storage system are switched after a short time to the WORM status and thus protected against further changes or deletion if ESM is activated. A document located in the archiving folder is labelled with the attribute "R" after archiving in an existing Windows environment. The attribute "R" stands for Read only and activates the system's write protection for the document.

A time stamp is also generated by the program, which indicates the date of archiving and the retention period and ensures traceability.

In the audit procedures carried out for this purpose on the test system provided, the data filed was taken over and archived completely and correctly in all test cases with various folder structures and configurations. We were unable to carry out any changes to the documents within the archiving period that was set.

3.5.1.3 Immutability of the documents

The documents are protected against the possibility of being changed as soon as the archiving processes described in 3.4.1.2 have been successful. The documents can no longer be renamed, changed or deleted after this process. Based on the audit procedures that we conducted, it was not possible to find any indication that the security settings or the write protection can be circumvented. None of the configuration changes to the storage system that were conducted were taken over, and they thus confirmed the immutability. It is possible to delete the documents after the retention period has expired. However, renaming or changing the document is still not permitted. During the attempt to change or delete documents, known Windows error messages appear that refuse access to the files.

The deletion of the documents was also verified as part of the audit. Furthermore, changes to and renaming and deletion of the documents during and after the term as well as the circumvention of the write protection were audited. The immutability of the documents within the storage system is guaranteed in due consideration of the encryption method and fulfils the requirements placed on the software.

3.5.1.4 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 throughout the retention period 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

General terms and conditions of engagement for auditors and auditing companies as amended on 1 January 2017.

[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, 2017

1. Scope of application

(1) These engagement terms apply to contracts between German Public Auditors (*Wirtschaftsprüfer*) or German Public Audit Firms (*Wirtschaftsprüfungsgesellschaften*) – hereinafter collectively referred to as ”German Public Auditors” – and their engaging parties for assurance services, tax advisory services, advice on business matters and other engagements except as otherwise agreed in writing or prescribed by a mandatory rule.

(2) Third parties may derive claims from contracts between German Public Auditors and engaging parties only when this is expressly agreed or results from mandatory rules prescribed by law. In relation to such claims, these engagement terms also apply to these third parties.

2. Scope and execution of the engagement

(1) Object of the engagement is the agreed service – not a particular economic result. The engagement will be performed in accordance with the German Principles of Proper Professional Conduct (*Grundsätze ordnungsmäßiger Berufsausübung*). The German Public Auditor does not assume any management functions in connection with his services. The German Public Auditor is not responsible for the use or implementation of the results of his services. The German Public Auditor is entitled to make use of competent persons to conduct the engagement.

(2) Except for assurance engagements (*betriebswirtschaftliche Prüfungen*), the consideration of foreign law requires an express written agreement.

(3) If circumstances or the legal situation change subsequent to the release of the final professional statement, the German Public Auditor is not obligated to refer the engaging party to changes or any consequences resulting therefrom.

3. The obligations of the engaging party to cooperate

(1) The engaging party shall ensure that all documents and further information necessary for the performance of the engagement are provided to the German Public Auditor on a timely basis, and that he is informed of all events and circumstances that may be of significance to the performance of the engagement. This also applies to those documents and further information, events and circumstances that first become known during the German Public Auditor’s work. The engaging party will also designate suitable persons to provide information.

(2) Upon the request of the German Public Auditor, the engaging party shall confirm the completeness of the documents and further information provided as well as the explanations and statements, in a written statement drafted by the German Public Auditor.

4. Ensuring independence

(1) The engaging party shall refrain from anything that endangers the independence of the German Public Auditor’s staff. This applies throughout the term of the engagement, and in particular to offers of employment or to assume an executive or non-executive role, and to offers to accept engagements on their own behalf.

(2) Were the performance of the engagement to impair the independence of the German Public Auditor, of related firms, firms within his network, or such firms associated with him, to which the independence requirements apply in the same way as to the German Public Auditor in other engagement relationships, the German Public Auditor is entitled to terminate the engagement for good cause.

5. Reporting and oral information

To the extent that the German Public Auditor is required to present results in writing as part of the work in executing the engagement, only that written work is authoritative. Drafts are non-binding. Except as otherwise agreed, oral statements and explanations by the German Public Auditor are binding only when they are confirmed in writing. Statements and information of the German Public Auditor outside of the engagement are always non-binding.

6. Distribution of a German Public Auditor‘s professional statement

(1) The distribution to a third party of professional statements of the German Public Auditor (results of work or extracts of the results of work whether in draft or in a final version) or information about the German Public Auditor acting for the engaging party requires the German Public Auditor’s written consent, unless the engaging party is obligated to distribute or inform due to law or a regulatory requirement.

(2) The use by the engaging party for promotional purposes of the German Public Auditor’s professional statements and of information about the German Public Auditor acting for the engaging party is prohibited.

7. Deficiency rectification

(1) In case there are any deficiencies, the engaging party is entitled to specific subsequent performance by the German Public Auditor. The engaging party may reduce the fees or cancel the contract for failure of such subsequent performance, for subsequent non-performance or unjustified refusal to perform subsequently, or for unconscionability or impossibility of subsequent performance. If the engagement was not commissioned by a consumer, the engaging party may only cancel the contract due to a deficiency if the service rendered is not relevant to him due to failure of subsequent performance, to subsequent non-performance, to unconscionability or impossibility of subsequent performance. No. 9 applies to the extent that further claims for damages exist.

(2) The engaging party must assert a claim for the rectification of deficiencies in writing (*Textform*) [*Translators Note: The German term “Textform” means in written form, but without requiring a signature*] without delay. Claims pursuant to paragraph 1 not arising from an intentional act expire after one year subsequent to the commencement of the time limit under the statute of limitations.

(3) Apparent deficiencies, such as clerical errors, arithmetical errors and deficiencies associated with technicalities contained in a German Public Auditor’s professional statement (long-form reports, expert opinions etc.) may be corrected – also versus third parties – by the German Public Auditor at any time. Misstatements which may call into question the results contained in a German Public Auditor’s professional statement entitle the German Public Auditor to withdraw such statement – also versus third parties. In such cases the German Public Auditor should first hear the engaging party, if practicable.

8. Confidentiality towards third parties, and data protection

(1) Pursuant to the law (§ [Article] 323 Abs 1 [paragraph 1] HGB [German Commercial Code: *Handelsgesetzbuch*], § 43 WPO [German Law regulating the Profession of Wirtschaftsprüfer: *Wirtschaftsprüferordnung*], § 203 StGB [German Criminal Code: *Strafgesetzbuch*]) the German Public Auditor is obligated to maintain confidentiality regarding facts and circumstances confided to him or of which he becomes aware in the course of his professional work, unless the engaging party releases him from this confidentiality obligation.

(2) When processing personal data, the German Public Auditor will observe national and European legal provisions on data protection.

9. Liability

(1) For legally required services by German Public Auditors, in particular audits, the respective legal limitations of liability, in particular the limitation of liability pursuant to § 323 Abs. 2 HGB, apply.

(2) Insofar neither a statutory limitation of liability is applicable, nor an individual contractual limitation of liability exists, the liability of the German Public Auditor for claims for damages of any other kind, except for damages resulting from injury to life, body or health as well as for damages that constitute a duty of replacement by a producer pursuant to § 1 ProdHaftG [German Product Liability Act: *Produkthaftungsgesetz*], for an individual case of damages caused by negligence is limited to € 4 million pursuant to § 54 a Abs. 1 Nr. 2 WPO.

(3) The German Public Auditor is entitled to invoke demurs and defenses based on the contractual relationship with the engaging party also towards third parties.

(4) When multiple claimants assert a claim for damages arising from an existing contractual relationship with the German Public Auditor due to the German Public Auditor's negligent breach of duty, the maximum amount stipulated in paragraph 2 applies to the respective claims of all claimants collectively.

(5) An individual case of damages within the meaning of paragraph 2 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 regardless of whether the damages occurred in one year or in a number of successive years. In this case, multiple acts or omissions based on the same source of error or on a source of error of an equivalent nature are deemed to be a single breach of duty if the matters in question are legally or economically connected to one another. In this event the claim against the German Public Auditor is limited to € 5 million. The limitation to the fivefold of the minimum amount insured does not apply to compulsory audits required by law.

(6) A claim for damages expires if a suit is not filed within six months subsequent to the written refusal of acceptance of the indemnity and the engaging party has been informed of this consequence. This does not apply to claims for damages resulting from scienter, a culpable injury to life, body or health as well as for damages that constitute a liability for replacement by a producer pursuant to § 1 ProdHaftG. The right to invoke a plea of the statute of limitations remains unaffected.

10. Supplementary provisions for audit engagements

(1) If the engaging party subsequently amends the financial statements or management report audited by a German Public Auditor and accompanied by an auditor's report, he may no longer use this auditor's report.

If the German Public Auditor has not issued an auditor's report, a reference to the audit conducted by the German Public Auditor in the management report or any other public reference is permitted only with the German Public Auditor's written consent and with a wording authorized by him.

(2) If the German Public Auditor revokes the auditor's report, it may no longer be used. If the engaging party has already made use of the auditor's report, then upon the request of the German Public Auditor he must give notification of the revocation.

(3) The engaging party has a right to five official copies of the report. Additional official copies will be charged separately.

11. Supplementary provisions for assistance in tax matters

(1) When advising on an individual tax issue as well as when providing ongoing tax advice, the German Public Auditor is entitled to use as a correct and complete basis the facts provided by the engaging party – especially numerical disclosures; this also applies to bookkeeping engagements. Nevertheless, he is obligated to indicate to the engaging party any errors he has identified.

(2) The tax advisory engagement does not encompass procedures required to observe deadlines, unless the German Public Auditor has explicitly accepted a corresponding engagement. In this case the engaging party must provide the German Public Auditor with all documents required to observe deadlines – in particular tax assessments – on such a timely basis that the German Public Auditor has an appropriate lead time.

(3) Except as agreed otherwise in writing, ongoing tax advice encompasses the following work during the contract period:

a) preparation of annual tax returns for income tax, corporate tax and business tax, as well as wealth tax returns, namely on the basis of the annual financial statements, and on other schedules and evidence documents required for the taxation, to be provided by the engaging party

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

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

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

e) participation in petition or protest and appeal procedures with respect to the taxes mentioned in (a).

In the aforementioned tasks the German Public Auditor takes into account material published legal decisions and administrative interpretations.

(4) If the German Public auditor receives a fixed fee for ongoing tax advice, the work mentioned under paragraph 3 (d) and (e) is to be remunerated separately, except as agreed otherwise in writing.

(5) Insofar the German Public Auditor is also a German Tax Advisor and the German Tax Advice Remuneration Regulation (*Steuerberatungsvergütungsverordnung*) is to be applied to calculate the remuneration, a greater or lesser remuneration than the legal default remuneration can be agreed in writing (*Textform*).

(6) Work relating to special individual issues for income tax, corporate tax, business tax, valuation assessments for property units, wealth tax, as well as all issues in relation to sales tax, payroll tax, other taxes and dues requires a separate engagement. This also applies to:

a) work on non-recurring tax matters, e.g. in the field of estate tax, capital transactions tax, and real estate sales tax**;**

b) support and representation in proceedings before tax and administrative courts and in criminal tax matters;

c) advisory work and work related to expert opinions in connection with changes in legal form and other re-organizations, capital increases and reductions, insolvency related business reorganizations, admission and retirement of owners, sale of a business, liquidations and the like, and

d) support in complying with disclosure and documentation obligations.

(7) To the extent that the preparation of the annual sales tax return is undertaken as additional work, this includes neither the review of any special accounting prerequisites nor the issue as to whether all potential sales tax allowances have been identified. No guarantee is given for the complete compilation of documents to claim the input tax credit.

12. Electronic communication

Communication between the German Public Auditor and the engaging party may be via e-mail. In the event that the engaging party does not wish to communicate via e-mail or sets special security requirements, such as the encryption of e-mails, the engaging party will inform the German Public Auditor in writing (*Textform*) accordingly.

13. Remuneration

(1) In addition to his claims for fees, the German Public Auditor is entitled to claim reimbursement of his expenses; sales tax will be billed additionally. He may claim appropriate advances on remuneration and reimbursement of expenses and may make the delivery of his services dependent upon the complete satisfaction of his claims. Multiple engaging parties are jointly and severally liable.

(2) If the engaging party is not a consumer, then a set-off against the German Public Auditor's claims for remuneration and reimbursement of expenses is admissible only for undisputed claims or claims determined to be legally binding.

14. Dispute Settlement

The German Public Auditor is not prepared to participate in dispute settlement procedures before a consumer arbitration board (*Verbraucherschlichtungsstelle*) within the meaning of § 2 of the German Act on Consumer Dispute Settlements (*Verbraucherstreitbeilegungsgesetz*).

15. Applicable law

The contract, the performance of the services and all claims resulting therefrom are exclusively governed by German law.