EBNER
STOLZ

Report

concerning the compliance of the
software product Therefore™ V. 17.2.1
with the data protection requirements
stipulated by the new EU General Data Protection Regulation (EU GDPR)

Therefore Corporation GmbH

Mödling, Austria

2017

2017-2-1063

Ebner Stolz GmbH & Co. KG

Wirtschaftsprüfungsgesellschaft Steuerberatungsgesellschaft
Stuttgart

EBNER STOLZ

Contents

Appendices

EBNER
STOLZ

A. Engagement and performance of activities

We were instructed by the management of Therefore Corporation GmbH, Mödling, Austria (hereinafter referred to as "Therefore" or the "Company") to review Version V 17.2.1 of the software known as Therefore™ to determine whether it can be operated in accordance with the data protection conformity requirements set out in the "Regulation of the European Parliament and Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC" ("General Data Protection Regulation" or "EU GDPR").

Therefore is a comprehensive enterprise content management (ECM) software solution for the enterprise-wide recording, management and archiving of all kinds of documents. With these functions it is possible to store and manage documents and information in a structured information management process and make them available for reading at the relevant places.

Any personal data contained in the documents and information processed by Therefore is subject to the data protection requirements provided for in EU GDPR. The term "personal data" is defined in Article 4 of the EU GDPR and in Section 3 (1) of the German Federal Data Protection Act. Under this definition, the term "personal data" refers to all information relating to an identified or identifiable natural person. A natural person is deemed to be identifiable if he can be identified directly or indirectly by reference to an ID, name, identity number, positioning data, online ID or any other special characteristics.

The General Data Protection Regulation (EU GDPR) was adopted by the European Union for the purpose of harmonizing the rules for processing personal data by private-sector and public-sector bodies across the EU. This aims to improve the protection of personal data within the European Union, while safeguarding the free movement of data within the European single market. EU GDPR is subject to compulsory application within the European Union from May 25, 2018.

Article 25 of the EU GDPR defines the requirements of "privacy by design" and "privacy by default". Generally speaking, software solutions are deemed to comply with data protection requirements if they observe the principles of "privacy by design", "privacy by default", the rule of data minimization, the observance of potential duties to delete data where necessary and the inclusion of suitable data protection tools within the software. The following specific criteria are decisive for implementation in the software solution or IT application:

- Distributed processing and storage of data
- Data aggregation
- Logging function to prove observance of requirements
- Scope for deleting data to observe the "right to be forgotten"
- Automatic deletion after expiry of the compulsory retention period
- Encrypted storage or transmission

- Authorization system to control access
- Storage and processing confined to necessary data
- Corresponding design of input dialog boxes
- Pseudonymization of data to prevent simple traceability
- Anonymization of data to prevent simple traceability
- Storage of data confined to the purpose for which it is processed
- Authentication and authentification

Type and scope of the audit with details of the individual steps and the results gained are set out in this report.

This engagement and our liability, also in relation to third parties, are governed by the "General Engagement Terms for Wirtschaftsprüfer and Wirtschaftsprüfungsgesellschaften" dated January 1, 2017, which are attached to this report as Appendix 1.

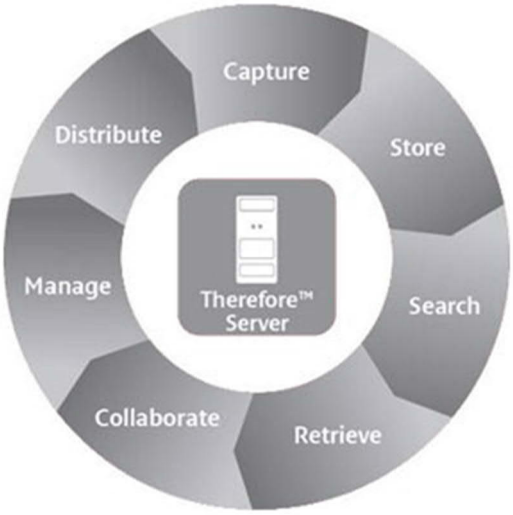
The audit was performed by inspecting documents, conducting testing in a test installation and interviewing the client. The main sources of information were the documentation provided and the online help as well as information provided by the responsible employees. More advanced efficacy reviews were outside the scope of the audit.

We documented the results of our audit activities in our working papers.

The audit was conducted on November 23-27, 2017 at Therefore's offices as well as at our own offices.

B. System description

Therefore™ is a comprehensive enterprise content management (ECM) software solution for the enterprise-wide recording, management and archiving of all kinds of documents. With these functions it is possible to store and manage documents and information in a structured information management process and make them available for reading at the relevant places. This also includes personal documents and information.



Therefore
PEOPLE PROCESS INFORMATION

:

In particular, Therefore™ links data capturing, storage, management and processing, unifies processes to boost production and creates internal workflows. Using Therefore™, it is possible to capture, manage, process and control all information, to archive it and to reproduce it at any time on an enterprise-wide basis at all locations regardless of the format and source.

Therefore™ information software makes it possible to collect information (either in electric or paper form) in many different ways. This can, for example, be done by an external scanner to capture a physical document or by means of connectors. Similarly, Therefore™ features a large number of interfaces with existing software products to ensure uncomplicated file management, particularly of individual Microsoft Office files. However, entire file structures can also be deposited directly in Therefore™.

As soon as Therefore has stored a file, it can be placed in the primary storage and optionally also in a backup storage to ensure that all data remains available in the event of any storage failure. Moreover, Therefore adds a digital signature to every document as soon as it is stored. This signature is changed whenever the file is accessed and modified, thus ensuring full traceability of the individual processing steps.

The software includes a user management system for managing the data. This permits different users or user groups to view or edit certain files or restricts their rights to do so, thus ensuring that processing of personal data conforms to the GDPR.

It is possible to create workflows individually in order to map processes within the enterprise with greater precision. These workflows transmit data independently within the enterprise to largely automate the process steps. This is also possible in connection with the direct transmission of messages to third parties outside the enterprise. Accordingly, it is also possible to send messages directly to third parties who are located outside the company. In this way, several persons can be automatically informed of a given process. It is also possible to define conditions determining when a given item of information is to be forwarded or what processes must be triggered in the event of any deviation from the standard process.

Moreover, statistics and analyses on these workflows can be created to detect the processes that exhibit potential for improvement. Therefore™ can create these automatically and display them graphically.

Details of audit results

With its Therefore™ software product, Therefore provides functions that appropriately support compliance with the data protection requirements that software products must satisfy under the EU GDPR.

In addition to a Therefore test installation, the following documentation was available to us for review:

- Therefore Security (documentation of security settings)
- The online help on the Company's website

The functions of the system which we inspected are appropriate for ensuring compliance with the data protection requirements for software solutions (e.g. with respect to "privacy by design" and "privacy by default"). The tests that we performed showed that the controls that had been implemented and activated function correctly and permit compliance with the principles of data protection applicable to the processing and archiving of personal data and information.

As is customary with standard software packages, material parts of the Therefore™ software product are configurable with respect to the activation and specific design of individual controls. It is also customary for only the coexistence and harmonization of technical and organizational measures to result in an individually appropriate control process and compliance with data protection requirements. In this connection, we wish to draw attention to what we consider to be the necessary measures for ensuring compliance with the data protection requirements provided for in EU GDPR in order for personal data and information to be processed in accordance with data protection requirements.

The term "processing" is defined in Article 4 of EU GDPR. Under this definition, processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1. Processing of personal data and information in accordance with data protection requirements

Distributed processing and storage of data

Personal data must be processed and stored on a distributed basis for the purposes of data protection. Steps must be taken to ensure that personal data collected and stored for different purposes is processed separately (Article 32 of the EU GDPR).

Therefore™ uses "categories" as a central concept. These are the main criterion for ordering data within the application and are characterized by a set of properties (general, default system-defined attributes) and descriptors (customer-specific attributes). The security and archiving settings must be defined separately for each category.

In addition, Therefore™ allows protection requirement classes to be defined for each category via a separate attribute to ensure that only limited groups of persons can access the documents in question. In this way, it is ultimately possible to implement the distributed processing of personal documents and information requiring special protection.

Each customer is able to individually create his own file structure in accordance with internally defined requirements.

Data aggregation

The principle of data aggregation calls for personal data to be grouped together for processing purposes (Article 5 of the EU GDPR).

Document management systems are not designed per se to evaluate or analyze the data that they hold. Even so, Therefore has a "business analytics" function for creating reports. In this connection, a distinction must be drawn between analytics using SQL and analytics using Power BI. Power BI analytics use solely internal data and indices.

Standard reports are defined for SQL and can also be extended by customers. These are based on index data or workflow process analyses. If only index data is processed and the default standard reports are used, no objections arise from a data protection point of view. However, SQL-based analyses also allow external databases to be included, allowing potential analyses that go beyond the original purpose for which the data was collected. It is consequently the software user's responsibility to ensure that only evaluations that comply with data protection legislation are carried out and that no data is processed without the consent of the persons concerned.

Encrypted storage

In order to protect the security of personal data and to prevent any unauthorized processing of it, EU GDPR stipulates that the data controller and the processor must identify the risks arising from the processing of the data and simultaneously implement steps, taking into account the state of the art, in order to minimize such risks. One such measure for protecting confidentiality is to encrypt personal data (Articles 32 and 35 of the EU GDPR).

Therefore™ signs all documents as soon as they have been stored. The signature is verified whenever the documents are retrieved. It includes the following:

- All pages of the document (tif, pdf, docx, ...)
- Time stamp
- Name of the Therefore™ server
- ID of the key used
- User ID of the person who performed the archiving
- Document number

The signature is stored in the ".thex" file and generated using a standard signature algorithm that calculates the SHA 256 hash and encrypts this hash value with the RSA algorithm.

Therefore™ generates an RSA key using the Microsoft® Crypt API. The private key is stored securely in the operating system and periodically recreated. The public key is stored in the Therefore™ database and is used to verify documents. If any changes are made to the .thex file and thus to the document at the file level, the user is warned that the signature is invalid when the document is opened.

In connection with the transport of documents, encryption is carried out on the client server using the Hypertext Transfer Protocol Secure (https) transmission protocol and thus encrypted.

In the Therefore™ default settings it is possible to define separate storage policies and assign them to the categories. These storage policies determine which categories are to be stored on which device (primary storage or backup storage). The default setting providing for documents to be stored in the "buffer" directory should be altered to define secure primary and backup storage sites. Therefore™ also offers the option of using NetApp's Snaplock technology. This must be done in the "Solution Designer" settings. Therefore™ does not have any encrypted storage technology of its own. Encrypted (e.g. using the Windows Encrypting File System (EFS)) permanent storage must be defined by setting the individual storage solution when Therefore™ is used.

Right to data portability

A data subject has the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format. In addition, the data subject has the right to transmit that data to another controller without hindrance from the controller to which the personal data has been provided (Article 20 of the EU GDPR).

In Therefore™ the personal documents and information available in the system on a given person may be displayed on a structured basis according to different search criteria and exported in the form of an XML file.

Model for access control, authorization and authentification

EU GDPR stipulates the implementation of suitable technical and organizational measures for ensuring the secure processing of personal data (Article 32 of the EU GDPR). These measures also include the possibility for safeguarding the confidentiality, integrity, availability and resilience of the systems and services in connection with processing on a sustained basis.

Only persons nominated in advance may exercise the rights assigned to them (e.g. searching for and exporting personal data) and process the data in question. The application software must ensure that, by issuing user IDs and passwords and by assigning rights to these individual user profiles, it allows only authorized employees to access certain functions and/or particularly sensitive personal data.

Access to the categories is determined by corresponding access rights. Therefore™ offers the possibility of creating a link with the Microsoft Windows "Active Directory" directory service, in which the structure of the enterprise (incl. structure and process organization) are mapped in order to directly replicate single and group allocations. In connection with the authorization concept, it is thus necessary to draw a distinction between uses that have been created internally in the Therefore™ system ("internal users") and those that have access via the Active Directory.

User administration in Therefore™ utilizes the "Solution Designer" and manages the internal users, i.e. the users and user groups created within the application both via the organizational structure and via the process organization. The organizational structure defined in Therefore™ can allocate certain units, e.g. accounting, to certain persons, e.g. accounts receivable management. By contrast, the procedural organization assigns groups, e.g. creating creditors, to the individual persons. The purpose of the application is to manage groups via the Active Directory in order to reduce additional resource requirements for administration.

Categories can be accessed via individual or group rights, with the individual rights normally overriding the group rights. In addition, dedicated authorizations (e.g. at the field level) can only be assigned within individual workflows that are prohibited outside the workflow. This means that it is possible to protect individual categories and sub-categories. In addition, it is possible to assign specific rights outside the roles if role-based concepts are no longer sufficient. These specific rights for special cases within workflows are stored in ".dll" files.

Password policies apply to user authentification during the login phase. If Windows or the link with the Active Directory is used, the software customers have a single-sign-on option, i.e. an automatic login to Therefore™ using the Windows credentials. The restrictions defined in the Active Directory also apply as password restrictions. If there is no link with the Active Directory, meaning that the password restrictions are not automatically applied, Therefore™ uses the following default parameter settings:

- Format
  - Password format: Defines the elements (upper case, lower case, number format, special characters) that a password may include. On the system side, at least three of the four criteria mentioned must be included in the password.
  - Minimum password length: The minimum number of characters for a valid password. A password for Therefore™ must consist of at least eight characters.
- Account
  - Maximum number of failed login attempts: Determines how many consecutive login attempts may fail before the user is locked out. Therefore™ permits five login attempts before locking the user out.

The Therefore™ authorization model and password policy ensures compliance with the EU GDPR requirements by issuing user IDs and passwords and assigning rights to these persons. In this way, they are only able to exercise the rights that have been assigned to them and access and process the archived personal documents and data in accordance with these rights. If there is a link with the Active Directory, the customer is responsible for implementing the necessary settings to ensure compliance with the technical requirements of the EU GDPR.

Storage and processing confined to necessary data

The EU GDPR principle of data minimization says that personal data should be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed (Article 5 of the EU GDPR).

Therefore™ is used as an ECM system for recording, managing and archiving documents of all kinds including personal data and information. Accordingly, it provides functions which support the above-mentioned process steps. Depending on the categories defined in advance, it is possible to determine which documents are to be entered and stored in the system and with what method. The documents that are actually placed in the system are determined by the individual user. The access rights defined in the authorization model can ensure that only competent users observing the principle of data minimization are able to process and store personal data and information in the system. In this connection, separate organizational precautions are required in addition to the technical measures provided by the system.

We recommend raising the awareness of employees responsible for processing personal data and information within the enterprise by means of training etc. This also applies to the administrators of the system used.

Storage of data confined to the purpose for which it is processed

The principle of purpose limitation stipulates that personal data may only be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is, in accordance with Article 89, not considered to be incompatible with the initial purposes (Article 5 EU GDPR).

Within the system, the available personal data and information is used solely for managing the documents stored in the ECM solution and for optimizing processes. The main focus is on rendering information available along the business processes. The system does not offer any other possibilities beyond this for evaluating or analyzing personal data.

Corresponding design of input dialog boxes

EU GDPR stipulates that the software solutions used must be able to support the observance of data protection requirements by design and by default (Article 25 of the EU GDPR).

The functions available in Therefore™ for users depend on the specific rights that have been assigned to them. Accordingly, the scope for entering data and the design of the input dialog boxes depend on the step to be performed in the system and the appropriate authorization. Each customer or user with the appropriate rights is able to determine which data fields are to be saved in connection with the document. In this connection, we recommend that the users and operators of the system should take organizational precautions to ensure that the authorization model is suitable for achieving the requisite degree of protection of the personal data available. The organizationally defined authorization concept can be mapped to the customer's Active Directory via the linking options as well as to Therefore™ itself on the system side.

Pseudonymization and anonymization of data to prevent simple traceability

The principle of pseudonymization and anonymization of data to prevent simple traceability calls for personal data to be pseudonymized and anonymized for processing purposes. The purpose of this is to prevent the data subject from being identified when the personal data undergoes further processing (Articles 25 and 32 of the EU GDPR).

We also refer in this section to the comments that we have made on "data aggregation". SQL-based analyses allow external databases to be included and thus to be linked with data, enabling potential analyses that go beyond the original purpose for which the data was collected. Consequently, it is the customer's responsibility to ensure that only evaluations that comply with data protection legislation are carried out and that no data is processed without the consent of the person concerned.

This requirement does not apply to Therefore™ as long as the default analytics using SQL or Power BI are used.

2. Archiving of personal data and information in accordance with data protection requirements

Archiving periods, scope for deleting data to observe the "right to be forgotten", possibility of automatic deletion

Article 17 of the EU GDPR stipulates that the data subject has the right to ask the controller to erase his or her personal data without undue delay and that the controller has the obligation to erase personal data without undue delay under certain circumstances.

At the same time, data, data records and electronic documents that are subject to compulsory collection and archiving and have arisen in or been received by the company must be archived in this form and may not be deleted before the expiry of the statutory retention period (Austria: Sections 131, 132 of the Austrian Federal Tax Code; Germany: Section 147 (1) of the German Tax Code, decision by the German Federal Tax Court of June 24, 2009). Accordingly, they may no longer be stored solely in printed form and must remain permanent for the duration of the retention period (e.g. invoices received by e-mail as a PDF file or scanned paper documents). These requirements apply to documents that are subject to specific statutory retention requirements (e.g. all commercial documents as well as documents relevant for tax purposes) regardless of whether they comprise personal data or not.

In practice, this means that personal data and information must be deleted by no later than the expiry of the statutory retention period. Moreover, technical and organizational measures must be taken to ensure compliance with data protection requirements when the data is entered as well as for the entire duration of the period in which it is archived.

Therefore™ can be configured to add to documents a precise date on which the retention period expires. The archiving periods are managed in the Solution Design under "Retention policies". In this way, it is possible to determine whether a document is to be retained or deleted upon the expiry of the retention period.

Retention policies are assigned to a category on a 1:n basis – i.e. a retention policy can be assigned to multiple categories. A category cannot have more than one retention policy. By defining subcategories within categories, it is possible to assign different retention policies to individual subcategories. The following main information is stored in a retention policy:

– Length of retention period

The number of months defined for this policy determines the duration for which an assigned document is archived before being deleted.

– Criteria for determining the length of the retention period

This defines the criterion for the commencement of the retention period. The retention period can be measured

- on the date of creation,
- on the date of last modification, or
- on an individually defined date in the index field.

If the minimum retention period has expired, this does not mean that the documents concerned are automatically deleted. If documents are available for deleting, the administration must trigger a manual process to delete them. This means that administration has an overview of what documents are available for deleting and can thus verify this. After the delete request is confirmed, a log file is placed in a defined directory to list the documents that have been deleted.

Therefore™ allows accounting documents to be archived for the statutory periods by means of strong or unlimited retention control. At the same time, it offers deletion options to ensure compliance with data protection requirements with respect to data subjects' rights.

The settings made in Therefore™ are crucial for managing the retention periods.

Logging function to prove observance of requirements

The principle of accountability means that the data controller must be able to prove that it has complied with the data protection requirements as defined in Article 5 (1) of the EU GDPR in connection with personal data.

The logging function is activated by default in Therefore™. This automatically logs all activities in connection with the deletion of documents for example. The "audit log level" is customizable to monitor each individual step in document processing as well as retention and deleting. The log can prove that documents containing personal information have in fact been deleted in accordance with the applicable requirements.

In addition, Therefore™ has an individual user authorization management system that determines which users or persons have what kind of access to personal data and information.

Logging can be activated on a selective basis. A general distinction is drawn between "document events", "workflow events", "task events" and "administration events". "Document events" include actions to add, retrieve, edit, export, delete and print documents. "Administration events" are particularly used for logging the server startup or shutdown as well as any changes to the security or other settings. There are different monitoring levels: "Log always", "Log failure", "Log success" and "Do not log". The main customizing settings such as the security settings, login and password changed (including an indication of what was changed) are logged. This detailed documentation is not available for all customizing settings (e.g. storage). Accordingly, the customer must take steps to ensure that any changes to the customizing settings are duly logged (including details of what was changed).

A log file is stored in a central storage location defined by the customer until it is archived by the system. As a compensatory check by the customer, steps must be taken to ensure that access to the directory is correspondingly restrictive in order to prevent any log files from being manipulated. In the settings it is possible to define when the log file is archived.

The audit log is configured in the Solution Designer. Changes to the server logging settings do not become immediately active. Instead, the Therefore server service must be restarted manually to activate the changes. It is important to bear this in mind to ensure that all changes are duly logged.

The logging function for individual document processing steps should always be activated. We recommend defining the log level on the basis of the degree of protection required for the personal data being managed.

EBNER
STOLZ

C. Result of audit

Based on our audit findings, the documents submitted, the information received and the inspection of the systems, we express the following opinion:

"To Therefore Corporation GmbH, **Mödling, Austria**

In our opinion based on the findings of our audit, the software product Therefore™ V 17.2.1 permits compliance with the data protection requirements for software solutions in accordance with the General Data Protection Regulation (EU GDPR), which came into force on May 24, 2016 and takes effect from May 25, 2018, provided that it is used correctly and in connection with specific organizational controls by the Therefore™ customer."

We confirm that this audit report has been translated from its original German form into English by an independent, third-party professional agency.

Cologne, November 28, 2017

Ebner Stolz GmbH & Co. KG
Wirtschaftsprüfungsgesellschaft Steuerberatungsgesellschaft

Holger Klindtworth
CIA, CISA, CISM

Thomas Heithausen
Wirtschaftsprüfer
(German public accountant)

Appendices

[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.