

Conditions for access

Conditions for getting access to the assurance engagement report of the assurance engagement regarding the appropriateness, implementation and effectiveness of the compliance management system (CMS) of T-Systems International GmbH for the effectiveness period from 1 April to 30 September 2020 for the delineated area of anti- corruption (confirmation date: 11 December 2020)

Deutsche Telekom AG engaged KPMG AG Wirtschaftsprüfungsgesellschaft (KPMG) to perform a reasonable assurance engagement regarding the appropriateness, implementation and effectiveness of the compliance management system of T-Systems International GmbH for the delineated area of anti-corruption. The CMS description, which is the basis of the assurance engagement, is attached to the assurance engagement report (Appendix 1).

The results of the assurance engagement were summarized within an assurance engagement report addressed to T-Systems International GmbH. We have carried out our engagement on the basis of the General Engagement Terms for German Public Auditors and Public Audit Firms included in our engagement agreement dated as of 1 January 2017.

[AAB \(PDF, English\) 57 KB](#)

Please note, that the following assurance engagement report was provided in fulfilment of a contractual agreement with Deutsche Telekom AG and that this version of the assurance engagement report may only be used in a tendering process.

I confirm that I take note of the content of the AAB and that I would like to get access to the following assurance engagement report on that basis.



Assurance engagement of the compliance manage- ment system, delineated area of anti-corruption

TRANSLATION - ASSURANCE ENGAGEMENT REPORT

T-Systems International GmbH
Frankfurt am Main

Assurance engagement regarding the appropriateness, implementation and effectiveness of the compliance management system of TSI as of September 30, 2020, for the delineated area of anti-corruption

KPMG AG Wirtschaftsprüfungsgesellschaft

The English language text below is a translation provided for information purposes only. The original German text shall prevail in the event of any discrepancies between the English translation and the German original. We do not accept any liability for the use of, or reliance on, the English translation or for any errors or misunderstandings that may arise from the translation.

Table of Contents

1	Assurance engagement	1
2	Definition and delineation of the compliance management system	2
3	Performance of the engagement	3
3.1	Subject of the engagement	3
3.2	Nature and scope of review procedures	4
4	Findings and recommendations for the compliance management system	8
4.1	Findings for the compliance management system	8
4.2	Recommendations for the compliance management system	12
5	Assurance opinion	15

Appendices

Description of the Compliance Management System of Deutsche Telekom	1
General Engagement Terms	2

To T-Systems International GmbH, Frankfurt am Main, Germany

1 Assurance engagement

With purchase order from February 7, 2020 Deutsche Telekom AG (hereafter “DTAG”) engaged us to perform a reasonable assurance engagement on the attached description (Appendix 1) of the appropriateness, implementation and operating effectiveness of the compliance management system (hereafter “CMS description”) for the delineated area of anti-corruption of DTAG and 22 of its subsidiaries and affiliates (hereafter “Deutsche Telekom”). This report only refers to the audit of the compliance management system for the delineated area of anti-corruption during the period of operating effectiveness from April 1 to September 30, 2020 of

T-Systems International GmbH, Frankfurt am Main, Germany

– hereafter “TSI” or “entity” –.

This assurance report is intended for T-Systems International GmbH for informational purposes and may not be used in any other context than to inform TSI’s Board of Management or Supervisory Board. In particular, this assurance report may not be disclosed to third parties or used in sales brochures or other similar public documents or media unless our approval is given. We approve the transfer of this document to third parties, provided they acknowledge our limitation of liability in an electronically based counter-confirmation process or similar procedure. Third parties within the meaning of these regulations exclude members of the Supervisory Board. Our assurance report references the underlying engagement and terms agreed herein.

We have provided the services described above for TSI. We have carried out our engagement on the basis of the General Engagement Terms included in our engagement agreement dated as of January 1, 2017 (Appendix 2). By taking note of and using the information as contained in our assurance report, each recipient confirms to have taken note of the terms and conditions stipulated in the aforementioned General Engagement Terms (including the liability limitations specified in item no. 9 included therein) and acknowledges their validity in relation to us.

2 Definition and delineation of the compliance management system

A compliance management system (CMS) includes the principles and measures of an entity that are intended to ensure compliance of the entity, its employees and any third parties (if applicable), i.e. compliance with specific rules and requirements and/or the prevention of material violations of rules and requirements in clearly defined specific areas (non-compliance).

The design of a CMS includes specific generally accepted basic elements:

- the encouragement of a compliance culture,
- the design of the compliance framework (organizational and operational structure),
- the establishment of compliance objectives,
- the process for determining and analyzing compliance risks by the entity,
- the process of preparing the compliance program,
- the development of the communication process as well as
- the procedures for monitoring and improving the CMS.

A CMS is appropriate when it is suitable for both identifying in due time with reasonable assurance the risks of material non-compliance and for preventing such non-compliance. An appropriate CMS also ensures that incidences of non-compliance that have already occurred are reported promptly to the responsible unit in the entity so that the necessary actions for improving the CMS can be determined.

Even a CMS that has been appropriately designed and effectively implemented cannot absolutely ensure that the regulations of the delineated area will always be fulfilled or that non-compliance will be prevented, detected and sanctioned by the system. These inherent limitations of such systems result from the possibility that human judgement may lead to erroneous decision-making processes, that management may decide not to implement measures when costs exceed benefits, that disruptions solely due to simple human errors or mistakes may occur or that controls may be circumvented or overridden by two or more people in collusion.

3 Performance of the engagement

3.1 Subject of the engagement

The subject of our assurance engagement were the assertions contained in the CMS description in Appendix 1 regarding the appropriateness, implementation and operating effectiveness of the CMS of TSI for the delineated area of anti-corruption.

The legal representatives established its compliance program based on the frameworks set out in IDW AssS 980, ISO 19600, Australian Standard AS 3806-2006 and "ComplianceProgramMonitor" by ZfW ("Zentrum für Wirtschaftsethik", The Centre for Business Ethics). In accordance with our engagement letter, our engagement and reporting are limited to the rules of the CMS related to the delineated area of anti-corruption as described in the CMS description (Appendix 1):

"Deutsche Telekom sees corruption as being any type of conduct that is punishable by law in accordance with the following regulations: §§ 108e, 299 et seqq. and 331 et seqq. of the German Criminal Code, UK Bribery Act, US Foreign Corrupt Practices Act (FCPA), as well as criminal law provisions of other foreign legal systems that correspond with the content of the above."

Deutsche Telekom AG sets out minimum standards that apply across the Group for the design of the CMS. In accordance with a risk-oriented maturity model, the individual subsidiaries and affiliates are grouped into clusters, based on various parameters and data, and must gradually – depending on the cluster – fulfill increasing minimum requirements.

The entity's legal representatives are responsible for the CMS, including the CMS documentation and contents of the CMS description as well as the development and implementation of the associated principles and measures.

Our responsibility is to express an assurance opinion on the assertions made by the legal representatives in the CMS description (Appendix 1) about the appropriateness, implementation and effectiveness of the CMS for the delineated area of anti-corruption, on the basis of our engagement work.

A CMS is appropriate when it is suitable for both, identifying in due time with reasonable assurance the risks of material non-compliance and for preventing such non-compliance. An appropriate CMS also ensures that incidences of non-compliance that have already occurred are reported promptly to the responsible unit in the entity so that the necessary actions for improving the CMS can be determined.

The CMS is considered to be effective when the persons concerned acknowledge and comply with the principles and measures in ongoing business processes in accordance with their responsibility.

As a systems-related engagement, the objective of the assurance engagement is not to identify individual incidences of non-compliance. Therefore, it is not directed towards obtaining assurance about the actual compliance with regulations and requirements.

3.2 Nature and scope of review procedures

We performed our assurance engagement based on the professional duties set forth for public auditors as prescribed by the IDW Assurance Standard: Principles for the Proper Performance of Reasonable Assurance Engagements Relating to Compliance Management Systems (IDW AssS 980). This standard requires that we plan and perform the assurance engagement so that we can, with reasonable assurance, assess

- that the assertions contained in the CMS description regarding the principles and measures of the CMS are appropriately presented in all material respects,
- that the assertions contained in the CMS description about the CMS principles and measures are, in accordance with the applied CMS principles, suitable for both identifying in due time and with reasonable assurance risks of material non-compliance with corruption regulations and for preventing such non-compliance and
- that the principles and measures were implemented as of April 1, 2020 and were effective during the period from April 1 to September 30, 2020.

An adequate presentation includes statements covering all basic elements of a CMS and statements that do not contain any false information, inappropriate generalizations or unbalanced or biased presentations which may have the effect of misleading the addressees of the report.

We applied professional judgment in determining audit procedures during the assurance engagement. We considered our knowledge of the legal and economic environment as well as the compliance requirements of the maturity model of the Deutsche Telekom AG for the subsidiaries and affiliates. We assessed the principles and measures set forth in the CMS description and the evidence presented to us primarily on a sample basis. We believe that our engagement provides a reasonable basis for our assurance opinion.

The CMS of Deutsche Telekom is designed and rolled-out by the department Group Compliance Management. Therefore, our audit procedures on the appropriateness of the overall design concept and the effectiveness of processes carried out centrally were performed at central level (DTAG). In addition to the central compliance department (“Group Compliance Management”), Compliance Officers are designated at subsidiary level, who are responsible for implementing the CMS at the level of the subsidiary. Thus, audit procedures were also performed at the level of TSI.

At **central level** (DTAG) we performed the following audit procedures:

- Analysis of business activities in order to determine the resulting risks with respect to violation of anti-corruption regulations,
- Review of the CMS description,
- Review of the conceptual documentation of the maturity model of Deutsche Telekom,
- Review of board approvals and communication of compliance related policies, in particular Code of Conduct, Anti-Corruption Policy and Policy on the Acceptance and Granting of Benefits,
- Review of fundamental CMS documentation, e.g. process manuals and policies,
- Review of documents with regard to the design as well as the performance of the Compliance Risk Assessment in order to assess and validate the performed risk assessment with regard to corruption risks,
- Review of documentation regarding the organizational and operational structure of Group Compliance Management, i.e. rules of procedure for the Compliance Committee,
- Review of other organizational documents, such as minutes and reports on meetings,
- Review of documentation regarding the compliance communication, in particular compliance related communication by management (“tone from the top”) and compliance communication on the intranet,
- Inspection of IT-tools and portals, e. g. case management and consultation desk,
- Review of the design and performance of relevant ICS controls in procurement,
- Performance of random sample testing of the design and operating effectiveness of compliance-relevant measures and controls in the following business processes:
 - Procurement,
 - Events,
 - Donations,
 - Sponsoring,
 - M&A.

The business processes described above and the compliance relevant measures and controls contained therein refer to both DTAG and TSI. The basic populations for the random sample testing also included transactions and activities by TSI.

Furthermore, we conducted interviews at **central level** (DTAG) with the following representatives:

- Members of the Board of Management of DTAG,
- Executives and employees of the department Group Compliance Management,
- Executives and employees of the internal audit function,
- Executives and employees of other business areas, in particular:
 - Procurement,
 - HR,
 - Corporate Communications and
 - Group Corporate Responsibility.

At **decentral level** (TSI) we performed the following audit procedures:

- Review of documentation regarding the organizational and operational structure of the Compliance department of the entity (e. g. organizational charts, process manuals),
- Review of the documentation on the performance of the Compliance Risk Assessment regarding the assessment of corruption related risks,
- Review of documentation regarding the compliance communication, in particular compliance related communication by management (“tone from the top”) and compliance communication on the intranet of the entity,
- Review of board approvals and communication of compliance related policies, in particular Code of Conduct, Anti-Corruption Policy and Policy on the Acceptance and Granting of Benefits,
- Review of documentation regarding the handling of compliance tip-offs,
- Performance of random sample testing of the operating effectiveness of classroom trainings and the documentation of the participation in classroom trainings,
- Review of the design and performance of relevant ICS controls in sales as well as
- Performance of random sample testing of the operating effectiveness of key compliance controls in the sales process.

Furthermore, we conducted interviews at **decentral level** (TSI) with the following representatives:

- Compliance Officer and employees of the compliance department,
- Employees of other business areas, in particular sales, as well as
- Member of the TSI management board with overall compliance responsibility.

We performed the engagement (with interruptions) from February to December 2020.

We were provided with all the information and evidence we had requested. Legal representatives have provided a written representation on the completeness and accuracy of the CMS description and the explanations and evidence provided to us related to the appropriateness, implementation and effectiveness of the CMS.

4 Findings and recommendations for the compliance management system

4.1 Findings for the compliance management system

Without limiting our assurance opinion, we identified the following **findings** during our assurance engagement on the compliance management system of T-Systems International GmbH for the delineated area of anti-corruption.

The findings listed below were identified in the course of audit procedures performed at central level (DTAG), which are relevant for TSI. Therefore, they refer to business processes that lie within the central responsibility of DTAG.

Compliance-Program: Integrity checks of new suppliers

The global procurement policy stipulates that all suppliers must undergo an onboarding and qualification process before a business relationship is established. This includes in any case validating that the supplier is not included in the Non-Compliant List (a collection of all blacklists of the DT Group). For all potential new external suppliers, further supplier reviews have to be performed on a case-by-case basis, which are further specified in the chapter “Integrity Check” of the process manual. Accordingly, new suppliers have to complete a supplier questionnaire if the expected purchase volume exceeds EUR 100,000. The supplier questionnaire contains, inter alia, compliance-relevant questions. Depending on how the potential supplier answers the compliance questions, an assessment and approval by the procurement department “Compliance GSUS” is required. Following a risk-oriented approach, a Compliance Business Assessment (CBA) has to be obtained for new suppliers as well.

We performed random sample testing of the performance of integrity checks of new suppliers (4 transactions). Our sample testing resulted in the following finding:

- In three of the four selected samples a completed supplier questionnaire was not available. Therefore, it was not possible to review whether any necessary approvals by Compliance GSUS were obtained. In one of the three cases the supplier could not be identified in the Quick Check carried out subsequently.

We recommend explicitly integrating the supplier questionnaire into the system workflow so that it is not possible to engage suppliers for which a completed supplier questionnaire is not available. This way, it can also be ensured that any necessary approval by Compliance GSUS is obtained.

Compliance-Program: Engaging sales agents and lobbyists

Group Compliance Management (GCM) is part of the SAP workflow for engaging sales agents and lobbyists as a “special approver”. Therefore, all orders in the product groups that are subject to the Policy on Avoiding Corruption Risks when Working with Consultants (Consultant Policy) must be approved by GCM in SAP. For the approval, GCM checks whether a Compliance Business Assessment (CBA) is available for the respective supplier. If a valid and uncritical CBA is available, the order is approved by GCM; otherwise a CBA is commissioned. Due to a change in the product group codes at the beginning of the year 2020, GCM was no longer included in the SAP workflow for orders in the product groups subject to the Consultant Policy. It was therefore possible to place orders in a highly critical product group without a valid CBA and without the approval by GCM. GCM identified and reported the system error at the end of April. Afterwards, GCM evaluated whether orders had been placed in a highly critical product group without a valid CBA for the supplier due to this error. This was not the case. The system error has been fixed and GCM has been part of the workflow again since mid-June.

We performed random sample testing of the process for engaging consultants (3 transactions). Our sample testing resulted in the following findings:

- In one of the three samples a CBA from 2016 was available. CBAs are valid for 3 years. Therefore, the CBA had expired and not been renewed before the new order was placed. Possible newly arisen compliance-risks could therefore not be considered.
- In one of the three samples the consultant checklist, which has to be completed according to the Consultant Policy, was not available. The purpose of the consultant checklist is to check whether it is necessary to involve GCM.
- In one of the three samples the consultant checklist, which contains questions about the respective order, was available for a previous order in January 2019. The consultant checklist had not been filled out for the new order.

As part of the random sample testing two additional transactions from the product group “management consulting” were examined. When this product group is selected, the checklist Consultancy Services has to be completed in order to verify that the correct product group was selected. According to the requirements, the checklist must be added to the shopping cart. In one of the two cases the checklist had not been added to the shopping cart.

We recommend communicating the requirements of the Consultant Policy on a regular basis in order to maintain employees’ awareness.

Compliance-Program: Performing events

Requirements regarding the planning and performance of events are included in the Event Policy. Events are currently documented either via the EMC Tool or via the DTSE Event Tool. The DTSE Event Tool is intended to replace the EMC Tool in the future. The current version of the Event Policy only contains requirements related to the EMC Tool. Therefore, we recommend updating the Event Policy and also considering the DTSE Event Tool. The current approval processes focus on whether an event can be created and planned in principle. Compliance aspects are not considered. It is currently planned that the DTSE Event Tool, in which all events will be documented in the future, will include an approval process only for Telekom Deutschland GmbH. We recommend implementing controls within the approval process of events in order to reduce risks resulting from granting inappropriate benefits to third parties through events.

The external participants of events are not categorized when they are entered into the tools. Therefore, it is not possible to determine whether a participant is from the private or public sector. In case an event is also aimed at public officials, a separate approval by GCM is required according to the Policy on the Acceptance and Granting of Benefits. In the tool it can be specified whether the event is aimed at public officials as well. However, this field is not mandatory and it is up to the event organizer to obtain and document the necessary approval via Ask me!. We recommend actively asking whether the invited persons are public officials as part of the workflow. In addition, we recommend ensuring via the system that GCM is involved in these cases (e. g. by including a system-based lock that requires the upload of the compliance approval from Ask me! or alternatively by including GCM in the approval workflow in the system).

We performed random sample testing of the process for performing events (in total 12 transactions: 6 transactions from the EMC Tool, of which 3 had been cancelled, and 6 transactions from the DTSE Tool, of which 3 had been cancelled). Our sample testing resulted in the following findings:

- The DTSE Tool is designed to automatically change the status of an event to “post-editing” after the event date has passed. As a result, the event organizer receives a request to upload the necessary documents and to enter the participants of the event. Two of the six events from the DTSE Tool did not have the status “post-editing”, although the event date had already passed. The necessary documents were also not available.
- According to chapter 6.5.2 of the Event Policy, the (tax) relevant documents, e.g. the list of participants and the agenda, have to be uploaded in the tool by the event project manager within five working days after the end of the event. All other documents must be uploaded within three months after the end of the event. For two of the six events from the DTSE Tool, the documentation for the event had not been completed, although the event date had already passed (in some cases several months ago).

Compliance-Program: Performing sponsoring activities

The regulations for the performance of sponsoring activities are set out in the Sponsoring Policy. This policy defines which steps and approvals are required for the various types of sponsorings, e.g. brand-oriented sponsorings.

We performed random sample testing of the process for performing sponsoring activities (8 transactions). Our sample testing resulted in the following findings:

- According to chapter 5.7 of the Sponsoring Policy, sponsoring contracts are always prepared and/or reviewed in consultation with the responsible legal department. In two of the eight selected samples, the legal department was only involved by the department performing the sponsoring activity after conclusion of the contract.
- According to chapter 5.7 of the Sponsoring Policy, sponsoring contracts must always be concluded in written form and before any services are provided. For one of the two above mentioned samples, the sponsoring contract was signed after the sponsored event had already taken place.

We recommend communicating the requirements of the Sponsoring Policy to the responsible employees on a regular basis in order to maintain their awareness regarding the requirements.

4.2 Recommendations for the compliance management system

Again, without limiting our assurance opinion, we **recommend** the following for the delineated area of anti-corruption of the compliance management system of T-Systems International GmbH.

The recommendations listed below were identified in the course of audit procedures performed at central level (DTAG), which are relevant for TSI. Therefore, they refer to business processes that lie within the central responsibility of DTAG.

Compliance-Program: Control Element “Proper Ordering”

The Procurement Self-Assessment (ProSA) is used to test the effectiveness of the control element “Proper Ordering” of the Internal Control System. As part of ProSA, procurement transactions are checked on a sample basis and this check is documented in a ProSA Template.

In its current form, the ProSA Template contains questions that cannot be answered by the person completing the template because the answers cannot be verified. For instance, regarding proper ordering, the template contains the question, whether the approval workflow was followed and whether all approvals were obtained. However, the approvals cannot always be verified by the person completing the template since approvals are in some cases obtained and documented in preceding systems which the person completing the template does not have access to. As a result, the questions have currently been answered without a more in-depth review.

We recommend revising the ProSA Template and removing or adapting questions that cannot be verified and answered in their current form.

As an alternative, we performed random sample testing of the approvals required for purchase orders, which did not result in any findings.

Compliance-Program: Granting benefits

The Group Policy on the Acceptance and Granting of Benefits (Benefits Policy) defines cases, in which GCM has to be involved via Ask me! when benefits are accepted or granted, e. g. in case pre-defined value limits are exceeded. In certain cases, written approval from the supervisor is required additionally, e.g. when the employee is invited to events with a leisure component. In these cases, the benefit has to be documented in line with the requirements of the Benefits Policy (type of benefit, date of acceptance, value of the benefit etc.). Benefits to members of the public sector are generally not permitted, except for minor gifts with a total value of up to EUR 10. In all other cases, it is at the employee's discretion whether a benefit may be granted or accepted.

There are no specific requirements how the involvement of GCM in cases of doubt or exceptions should be documented. Employees have to document the benefits they granted and accepted themselves and manually. There is no superordinate or technically supported documentation of benefits that are granted or accepted. Therefore, it is not possible for GCM to monitor or review compliance with the requirements of the Benefits Policy.

We recommend specifying the requirements regarding the documentation of benefits that are accepted or granted. This can be done, for instance, by implementing a central documentation tool or by providing a template for documenting benefits (e.g. at team or department level). This way, it would also be possible for GCM to monitor or review compliance with the existing requirements.

Compliance-Program: Granting benefits via the “Ticketkalender”

The so called “Ticketkalender” is a tool that can be accessed by selected authorized persons who have been trained in this regard. These persons are eligible to order tickets from the sponsoring engagements of DTAG, e. g. for soccer matches of FC Bayern München, which externals can be invited to.

Currently, the Ticketkalender does not include an approval process. In addition, it does not intend any involvement of GCM. In the Ticketkalender it is not actively asked whether the invited person is a public official. In case public officials are invited, an approval via Ask me! is required, which should be uploaded in the Ticketkalender. However, there is no system-based lock in this respect which means that it is possible to invite public officials without the approval by GCM.

We recommend actively asking whether the invited persons are public officials as part of the workflow in the Ticketkalender. In addition, we recommend ensuring via the system that GCM is involved in these cases (e. g. by including a system-based lock that requires the upload of the compliance approval from Ask me! or alternatively by including GCM in the approval workflow in the system).

5 Assurance opinion

Our assurance opinion exclusively encompasses the CMS description of the delineated area of anti-corruption at T-Systems International GmbH, Frankfurt am Main. Any extrapolation or transfer of this assurance opinion to other compliance matters not covered by this delineated CMS area could lead to false conclusions being drawn.

Based on the findings of our reasonable assurance engagement we conclude that

- the assertions contained in the CMS description about the CMS principles and measures are appropriately presented in all material respects,
- the assertions contained in the CMS description about the CMS principles and measures are, in accordance with the applied CMS principles, suitable for both identifying in due time and with reasonable assurance risks of material non-compliance with corruption regulations and for preventing such non-compliance and
- the principles and measures were implemented as of April 1, 2020 and were effective during the period from April 1 to September 30, 2020.

For our detailed findings and recommendations, please refer to our statements in section 4 “Findings and recommendations for the compliance management system”. The CMS description for the delineated area of anti-corruption at the entity was completed as of September 30, 2020; the explanations of the assurance procedures for assessing the appropriateness, implementation and effectiveness of specific principles and measures cover the period from April 1 to September 30, 2020. Any extrapolation of this information to a future date could lead to false conclusions being drawn if the CMS has been changed in the interim.

Even an otherwise effective CMS is subject to inherent limitations of a system, which means that incidents of material non-compliance may occur that are not prevented or detected by the system. The objective of this assurance engagement is to obtain assurance on the system, not identifying any incidences of non-compliance. It is therefore not intended to obtain audit assurance on actual compliance with rules and regulations.

Duesseldorf, December 11, 2020

KPMG AG

Wirtschaftsprüfungsgesellschaft

[Original German version signed by:]

Stauder
Wirtschaftsprüfer
[German Public Auditor]

Quade
Steuerberaterin
[Certified Tax Consultant]

Appendices

Appendix 1
Description of the
Compliance Management
System of Deutsche
Telekom

Description of the Compliance Management System of Deutsche Telekom¹

Deutsche Telekom AG (DTAG) and its subsidiaries and affiliates (referred to below as DT) view compliance management as a holistic approach to minimizing compliance risks and ensuring adherence to company regulations. The Compliance Management System (CMS) described below outlines the measures and processes implemented as well as the associated objectives in terms of its basic elements, with the aim of ensuring compliance in the area of anti-corruption.

DT sees corruption as being any type of conduct that is punishable by law in accordance with the following regulations: §§ 108e, 299 et seqq. and 331 et seqq. of the German Criminal Code, UK Bribery Act, US Foreign Corrupt Practices Act (FCPA), as well as criminal law provisions of other foreign legal systems that correspond with the content of the above. DT established its compliance program on the basis of the frameworks set out in IDW AssS 980 (auditing standard of the Institute of Public Auditors in Germany), ISO19600, Australian Standard AS 3806-2006 and the ComplianceProgramMonitor by ZfW ("Zentrum für Wirtschaftsethik", The Centre for Business Ethics).

The description below serves as a basis for auditing DTAG and its subsidiaries and affiliates in accordance with IDW AssS 980.

The CMS sets out minimum standards that apply across the Group, however their implementation in the respective subsidiaries and affiliates is executed on a decentralized basis, depending on the CMS maturity model. With this model the individual subsidiaries and affiliates are grouped into clusters, based on various parameters and data, and must gradually – depending on the cluster – fulfill increasing minimum requirements (see also section "Compliance objectives").

Compliance culture

For DT it is particularly important that all employees, managers and corporate bodies conduct themselves in line with the company's values, adhere to applicable statutory regulations and follow internal rules at all times. According to DT's understanding Compliance entails more than the mere legitimacy of a company's actions. It is aimed at promoting the integrity of all employees by appealing for ethical, courageous and reflected behavior through the use of specific instruments, such as communication campaigns and training courses.

DT has a Code of Conduct that is used as a basic orientation framework for ensuring its people act with integrity and within the law. It bridges the gap between the Guiding Principles and the specific policies within the Group. The Code of Conduct

¹ In case of questions of understanding the German version is applicable.

applies worldwide to all employees, managers and corporate bodies within DT, and provides specific information on the behavior it expects from them in their daily work.

The importance of compliance and proper conduct is emphasized and communicated in regular Tone from the Top communications from the Board of Management and local managing boards. This is done through various channels, for example articles and videos in the Group intranet, or personal posts on the internal social network, e-mails to employees or through personal presentations and talks. The DTAG Board of Management uses personal statements to underline how important adherence to the rules is:

"For reliability, you need rules

But one thing we must not do – and this is probably more important now than ever – is bend the rules. We must not start doing things the wrong way. We adhere to the law. Always. And we follow the rules that we've agreed on for our collaboration.

Following the rules should be something that all of us take for granted. And something that requires no justification or explanation. This is what "compliance" is all about. We at Deutsche Telekom are not corrupt – nor are we corruptible. We always act ethically and honestly. That's the standard we follow. It's a standard that is right in line with our Guiding Principles. At our Group Headquarters, we've even gone so far as to engrave this idea in stone: "We are a trusted companion, whatever the circumstances."

Trust is more than just the basis for our business success. It's also the basis for our interactions with each other. To put this another way, those among us who always play by the rules are always on the safe side. We have no gray areas, and we don't look the other way, without speaking up, when rules are being broken. We don't have any slush funds, and we reject any and all misguided "esprit de corps."

Tim Höttges, CEO of Deutsche Telekom AG, June 2020, extract from a blog article titled "Dishonest behavior will never lead to honest business success" (published in DT intranet YAM).

The impact of the measures described on the compliance culture is measured by Group Compliance Management as part of the Group-wide employee survey and by the Group-wide survey on compliance based corporate culture.

Compliance objectives

To be the leading European telecommunications provider, DT wants to be seen by its customers as a reliable and ethical partner. Therefore, the aim is to prevent

compliance violations and non-ethical business decisions and to integrate compliance permanently into business processes at an early stage. Preventing and combating corruption has a key role to play here if the resulting high material and non-material damage (e.g., loss of trust) or unfair competition are to be avoided.

As previously mentioned, the CMS of DT is based on a maturity model. Maturity-oriented compliance management is based on the conviction that a group with a large number of different subsidiaries or affiliates needs customized compliance solutions for the relevant company. That is why gradually increasing minimum requirements for compliance management were defined for the subsidiaries/affiliates according to the commercial development and the exposure to risks. It has been precisely defined how the relevant compliance management is to be set up. As such, Group Compliance Management takes into account the fact that the size of the subsidiary/affiliate and different complexities, together with the risk characteristics of the business model, mean that requirements vary in terms of what CMS is appropriate. On this basis, the subsidiaries and affiliates are allocated to one of five clusters, each of which stipulates the compliance requirements to be met by them respectively. A review is carried out once a year on the allocation of a subsidiary/affiliate to a cluster. If necessary, the cluster is adapted and potential changes in requirements are assessed. An online tool is available to carry out the review.

Compliance risks

In order to systematically identify, analyze and evaluate compliance risks, and from this develop risk prevention measures, a Compliance Risk Assessment (CRA), which - as an overarching process - also covers DT subsidiaries and affiliates following risk-based scoping, is carried out by Group Compliance Management.

Group Compliance Management assists at a central level with its implementation and provides a standardized methodology. The aim behind this methodology is (1) that risks are evaluated with regard to likeliness and (2) magnitude of possible damage, (3) that risk management takes existing preventive measures into consideration, and (4) new compliance measures are derived for which clear responsibilities are assigned.

Group Compliance Management uses the findings of the CRA to derive Group-wide risk-based measures and inform the Board of Management and the Audit Committee of the DTAG Supervisory Board of the situation with regard to compliance risks within the Group. These measures form the basis of the Group Compliance Program, the implementation of which is regularly monitored by the Compliance Committee.

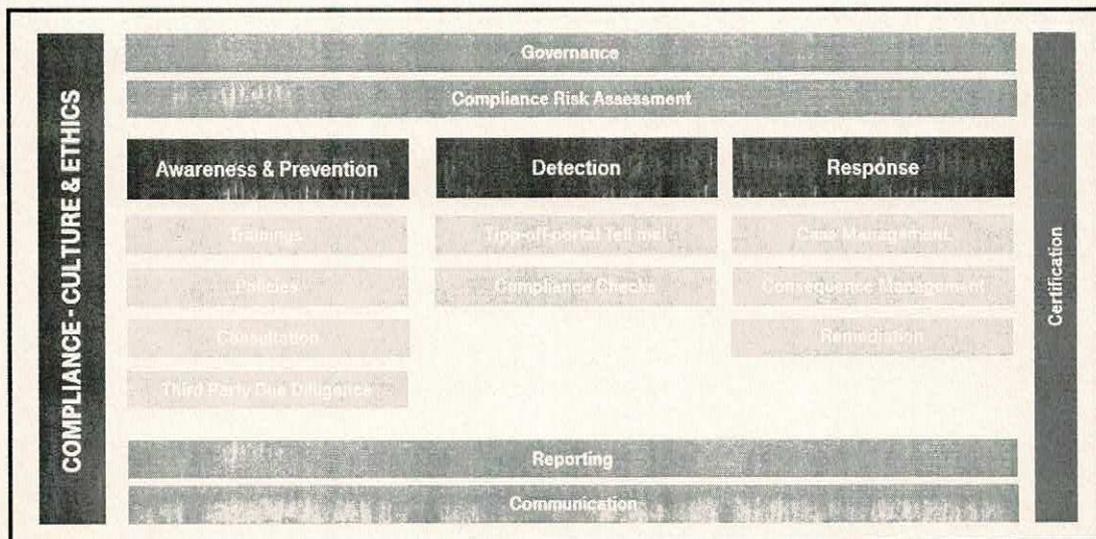
The purpose of subsidiary and affiliate participation in the CRA is to review and evaluate compliance on an individual basis against the backdrop of the company's objectives and respective business models.

The maturity model determines how often the subsidiaries/affiliates that are in scope of the CRA (yearly or every two years) should carry out the assessment and whether the standardized methodology should be used or whether deviations from it are possible. A tool is provided to allow the subsidiaries and affiliates to carry out the CRA based on the standardized methodology.

Compliance program

The implementation of overarching compliance goals in business activities is backed up by systematically applying the CMS in the areas of prevention, detection and response.

DEUTSCHE TELEKOM'S COMPLIANCE MANAGEMENT SYSTEM



Compliance Management System Deutsche Telekom

The basic elements – implemented in the subsidiaries and affiliates in various forms, depending on the cluster to which they are assigned – include:

- Compliance governance and organization (see Compliance organization)
- Compliance risk assessment (see Compliance risks)
- Reporting (see Compliance monitoring and improvement)
- Communication (see Compliance communication)
- Policies
- Training (see Compliance communication)
- Consultation desk
- Whistleblower portal
- Case management
- Business partner compliance

Policies: Group Compliance Management is responsible for policy management within the Group and supports the relevant specialist departments in implementing Group policies. The application and publication of policies is a binding process defined by Group Compliance Management.

The respective specialist departments are responsible for policy drafting, content and implementation. Group Compliance Management offers advice on the drafting and publication of policies. In addition, they work towards ensuring policies are reviewed and revised regularly. At the same time, they provide a centralized Group-wide policy database. This helps both policy owners to roll out new Group policies and employees to find the relevant policies.

DT has enforced various Group policies to combat corruption in the company. For all subsidiaries and affiliates – with the exception of those grouped in the lowest cluster – Group Compliance Management has defined two policies that need to be implemented ("Group Policy on the Acceptance and Granting of Benefits" and the "Group Policy on Avoiding Corruption Risks when Working with Consultants"). The maturity model also stipulates for each cluster what additional policies or regulations aimed at minimizing corruption-related risks are to be implemented in the subsidiaries or affiliates.

Consultation desk: To support employees with compliance-relevant behavioral uncertainties and to prevent any misconduct in advance, the compliance organization offers an advisory legal service to all employees – usually under the heading "Ask me!" – to ask compliance-related questions, for example regarding the Code of Conduct or compliance-relevant policies. Ask me! can be accessed using various communication channels (phone/e-mail) and is aimed at providing employees with a secure framework of proper conduct before violations can occur. The relevant Compliance Officers are involved should the handling of queries indicate towards systemic compliance risks and thus the need for action (e. g. trainings, awareness measures or – if permitted – further internal investigations).

Whistleblower portal: With the Tell me! whistleblower portal all external parties and employees have the opportunity to report compliance violations at any time, even anonymously. Individual subsidiaries or affiliates may offer local contact points for tip-offs that are known under a name that differs from "Tell me!"

Case management: DT has implemented a clearly defined case management process for systematically dealing with compliance-related cases and tip-offs:

- Group Compliance Management is responsible for ensuring the case management process is followed for cases relating to the Deutsche Telekom Group. As soon as there is an initial suspicion of misconduct, the case is passed on to the relevant decision-making body (e. g., Group Compliance Committee). They recommend which investigations and measures should be carried out. A case manager is responsible for the case documentation as well as for

- monitoring the progress of the case and drafting both status and final reports. Depending on the case concerned, the case manager may be a member of Group Compliance Management or of the investigating unit. In such cases Group Compliance Management monitors and documents the progress of the case using an IT-based documentation system (CMT).
- Cases which do not relate to the Group may be sent to the subsidiary or affiliate for processing. The subsidiaries have their own process based on that used at DTAG.
- Confirmed cases are sanctioned in line with national statutory regulations. Sanctions relating to labor law may range from talking to the respective employee to the termination of employment.

Alongside the processes that fall directly under Group Compliance Management, one of the tasks of the is to ensure compliance-related processes and checks are implemented in business operations too. In order that compliance is firmly anchored in business processes...

- ... a **Business Partner Compliance** approach has been implemented to ensure that compliance requirements are adhered to in the purchasing process. For example, contracts with suppliers generally include anti-corruption clauses. Also, voluntary e-learning courses are offered to help suppliers and business partners follow proper conduct rules. In addition, internal controls have been put in place, e.g., when approving consultants, for the operational procurement process or for identifying procurement bypasses. Furthermore, before contracts are concluded with new business partners, it is checked whether they are on the Group-wide 'Non-Compliant List.' In addition, risk-based background checks are carried out.
- ... relevant controls are implemented in the processes of initiating **sponsorships, events** and **donations** in order to minimize the risk of corruption.
- ... **sales processes** include controls that serve as a preventive means of limiting the risks of corruption. Firstly, a background check is made on all potential new sales partners based on set criteria. Also, controls are implemented regarding business relationships with external sales partners, e.g., when agreeing, verifying and approving credit notes, discounts and commissions.
- ... compliance rules are applied to **HR processes** at DT. Before an offer of employment is made, managers must submit a certificate of good conduct (or equivalent) as part of an integrity check provided that this does not contradict local laws. Applicants for high management positions go through an Assessment Center or structured interviews in which checks are made to see how closely matched the values of the applicant and company are. Compliance awareness-raising, e.g., in the form of online information or eLearning, is targeted at new employees as they are brought on board. Moreover, managers and selected
-

- members of staff are regularly assessed with regard to their conduct as part of their annual appraisal, with integrity a key criterion in the process.
- ... a compliance due diligence, based on set criteria, is performed as part of **M&A** projects, with the aim of identifying potential corruption risks in advance. The areas under examination include an analysis of the country-specific and business-related corruption risks, a review of the CMS and closed compliance cases relating to the organization being acquired. If a decision to integrate a company is taken, a defined process is to be followed.

Compliance organization

"Compliance organization" is the term used to describe the roles and responsibilities at all levels of the Group, from DTAG's Board of Management to the Compliance Officers in the relevant subsidiaries and affiliates. In addition to the central compliance unit, Compliance Officers are also appointed at the strategic business area and subsidiary/affiliate level. These are in charge of local implementation of the CMS and compliance objectives.

Following an organizational change at DTAG on January 2020 (dissolution of the board area Data Privacy, Legal Affairs and Compliance) the department Group Compliance Management was assigned to the area "Law & Integrity" (L&I) on April 1, 2020. The Chief Compliance Officer is heading the compliance department and has an organizational reporting line to the Head of L&I.

In order document tasks and responsibilities, so-called organizational profiles are used. Additionally, objectives, compliance tasks, reporting lines and participation opportunities of the Chief Compliance Officer are regulated in the business mandate of Group Compliance Management.

Central compliance organization

- The Chief Compliance Officer at DT and Group Compliance Management are responsible for the Group-wide structuring, enhancement, implementation and monitoring of the CMS.
- The Chief Compliance Officer leads the international compliance organization, is part of the Board area "Human Resources and Legal Affairs" and has the right to report to the Audit Committee of the DTAG Supervisory Board.
- DTAG has established a Compliance Committee, a cross-functional committee comprising representatives from e.g., HR, Legal, Internal Audit and other areas. It ensures there is a close exchange of information on all compliance-related issues and defines what procedure must be followed in the event of compliance violations.

Local compliance organization and responsibilities

- The same applies to defined subsidiaries or affiliates; responsibility for compliance is always assigned to a member of the top management.
- Also, local compliance officers are nominated in the operating segments and subsidiaries and affiliates. These are in charge of local implementation of the CMS and compliance targets.
- In order to meet their responsibilities all compliance officers have a clearly defined minimum pool of resources based on the areas for which they are responsible and the size of their subsidiary/affiliate, as well as the right to report to their respective supervisory bodies. He or she has a dotted line reporting relationship with the Chief Compliance Officer at DTAG or the compliance officer of the respective parent company, who agree an operational compliance target each year with the local compliance officers.
- At least subsidiaries and affiliates that are allocated to the highest cluster have compliance committee with a similar role to the above-mentioned DTAG committee.

To promote up-to-date compliance-related knowledge within the compliance organization, regular compliance-based courses and training sessions are offered to those responsible in both the central and local compliance organizations.

Collaboration with other specialist departments

Over and above this, regular, cross-functional exchanges take place between Group Compliance Management and other functions, including departments such as Internal Control System (ICS) and Internal Audit. Also, compliance-related matters are defined, reviewed and approved as part of regular ICS self-assessments.

Additionally, information on compliance risks provided by the compliance risk assessment process is systematically incorporated into the Internal Audit team's risk-based audit planning process.

Compliance communication

Communication is an integral component of the CMS. Its purpose is to inform, raise awareness and create a secure framework of proper conduct. At the same time DT is aiming to provide its external stakeholders with information, on a transparent basis, regarding the most significant developments, facts and figures around compliance issues.

To this end Group Compliance Management is developing a variety of measures, some of which are adopted by the subsidiaries and affiliated companies.

Examples of this include:

- Internal staff and manager communications (e.g., intranet, Telekom Social Network, posters, newsletters and video statements)
- Internal campaigns (topic-based, international awareness campaigns)
- Internal events (e.g., International Compliance Days)
- External communications (public relations, Internet)
- Investor communications (shareholders' meeting, inquiries from investors and rating agencies, CSR report)

The subsidiaries and affiliates are also free to develop their own communication formats.

The training concept is a key component of DT's CMS and provides for staff and management training. The courses offer training on compliance issues to the relevant target groups and communicate what DT's expectations are. The focus is placed on enhancing awareness of compliance risks at work and explaining in practical terms what ethical conduct conforming to the rules entails.

Classroom training or virtual training (e.g. in the form of Web-Ex conferences) covering anti-corruption and the basic principles of compliance is provided. The target groups are defined on a risk basis and are made up of executives, management teams as well as employees involved in high-risk processes in particular. The classroom-based courses are adapted to the requirements of the target groups and are updated at regular intervals. Classroom training takes place at least once every three years.

All employees are offered e-learning courses on anti-corruption and the fundamentals of compliance; participation in the courses is voluntary. In subsidiaries and affiliates that are allocated to the highest cluster target groups falling under the risk-based scope - such as, for example, Sales or Procurement - are specifically requested to complete the anti-corruption e-learning courses at least once every three years.

Furthermore, as a general rule all employees are offered the opportunity of self-learning on the intranet, where they can independently collect information and further their knowledge using various compliance-related intranet pages. Also, they can gain additional knowledge by conducting further voluntary e-learning courses.

Compliance monitoring and improvement

The implementation of the CMS is continuously monitored and adapted to developments within and outside of the company.

Both scheduled and situation-based reviews of the CMS are undertaken at a central level within DTAG. This is done in form of compliance checks and internal audits:

- **Compliance Checks** are local checks of business decisions and processes and are undertaken by Group Compliance Management in selected subsidiaries or affiliates, with the aim of increasing awareness of the relevance of compliance regulations. These checks are not based on tip-offs; they are systematic checks chosen on the basis of risk and serve to enhance the effectiveness of the CMS process. The objective here is to identify CMS deficits, process deficiencies or misconduct, and to derive measures to eliminate them.
- **Internal Audit** is responsible for defining the areas to be audited in its annual audit program. Compliance risks are also covered here. As previously mentioned, Group Compliance Management is involved in the planning of the audit program. These audits cover preventive as well as risk-based reviews, e.g., in connection with reported violations. Situation-based audits that are compliance-relevant may also be carried out. As a general rule, both the entire CMS and individual business processes may be reviewed for compliance. Measures relating to the CMS are implemented by the parties responsible in line with the action plan set out by Internal Audit.

Other measures related to **continuous monitoring**:

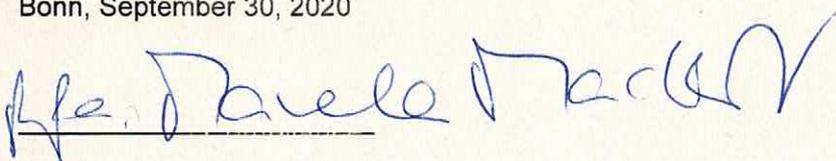
- **Reporting:** At Group level, quarterly reports on compliance-related issues are submitted to the Board of Management and the Audit Committee of the DTAG Supervisory Board. These reports include information on the enhancement of the CMS, relevant data, e.g., on training course participant numbers, compliance inquiry levels and information on major compliance violations. There are defined reporting lines and processes, from the subsidiary/affiliate level right up to the Group holding. The scope and frequency of compliance reporting, as well as the parties to whom these reports must be submitted, are defined at subsidiary/affiliate level.
- **Risk management functions:** Compliance requirements are documented as part of the ICS self-assessment process, and potential issues are dealt with by the subsidiaries or affiliates.

Additional **continuous improvement measures** include:

- DTAG has **external auditors** carry out regular audits to ensure the structure of the CMS is appropriate and it is being effectively implemented.

- Group Compliance Management is actively involved in various bodies and initiatives, such as for example the German Institute for Compliance (DICO) or the Forum Compliance & Integrity (FCI) and has regular exchanges with Compliance Officers of other DAX 30 companies. Facts and information from this are used to make suggestions and improvements for the CMS.

Bonn, September 30, 2020



Manuela Mackert
Chief Compliance Officer

Appendix 2
General Engagement
Terms

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.