New Developments in German Corporate Governance Law with Focus on Compliance and Data Protection Issues (GDPR)

Hans-Peter Marutschke

1. German Corporate Governance Code – changes in 2017

1.1 *Short introduction to the Code structure*

Although the German Corporate Governance Code ("The Code") is not a statutory law passed by parliament and belongs therefore to the category of "soft law", it has a legal basis in § 161 of the German Stock Corporations Act (AktG) through the mandatory "Declaration of conformity"[1], which has to be presented annually to the shareholders meeting and published on the corporate homepage, together with the year-end report and other documents.

1) § 161 AktG requires the following for the declaration of conformity:

(1) The executive board and supervisory board of the listed company shall declare annually that the recommendations of the "Deutscher Corporate Governance Kodex" (The Code) published by the Federal Ministry of Justice in the official section of the Federal Gazette have been and are being complied with or which of the Code's recommendations are not being applied and why. The same shall apply to the executive board and the supervisory board of a company which has exclusively issued other securities than shares for trading on an organized market in the sense of § 2 (5) of the Wertpapierhandelsgesetz [Securities Trading Act] and the issued shares of which shall, on the company's own initiative, only be traded via a multilateral trading facility in the sense of § 2 (3) sentence 1 No. 8 of the Wertpapierhandelsgesetz [Securities Trading Act].

(2) The declaration shall be permanently accessible to the public on the company's website.

The Code itself was established in September 2001 by a Commission, which had been introduced by the German Federal Minister of Justice and consists now of 14 managing and supervisory board representatives of German listed companies and their stakeholders, i.e. institutional and retail investors, academics (economics, jurisprudence), auditors and a trade union federation[2]. Once a year the Commission reviews the Code in order to find out, if it still describes the best practice of good corporate governance and adapts it when indicated.

There is still a widespread misunderstanding, especially in foreign countries, that this declaration of conformity has to cover everything mentioned in the Code. But in fact, it is of legal importance to distinguish two types of regulatory measures: recommendations and suggestions. Both are not mandatory, however, only deviations from the recommendations – not the suggestions – have to be explained and disclosed with the annual declaration of conformity (Comply or Explain). The recommendations and suggestions of the Code become valid with the publication in the official section of the Federal Gazette (Bundesgesetzblatt).

The Code explains in its foreword the difference between both types: Recommendations of the Code are indicated in the text by using the word "shall", suggestions are indicated in the text by using the word "should". The remaining passages of the code that do not use these words relate to descriptions of statutory requirements and explanations.

Besides giving recommendations and suggestions that reflect the best practice of corporate governance, the Code aims at enhancing the German corporate governance system's transparency and comprehensibility, in order

2) https://dcgk.de/en/kommission-33/members.html

to strengthen the confidence of international and national investors, clients, employees and the general public in the management and supervision of German listed companies.

1.2 *Changes introduced in 2017*

1.2.1 The "reputable businessperson"

Since its introduction in 2001 the Code has been amended 13 times, the latest amendment took place on February 7, 2017[3] after a two years unchanged period. As always, reasons for revision were manifold and mostly based on experiences of insufficiency discovered in practice or new developments in social discussion (like increasing women's quota in responsible positions in a company). It can be said, that this was also the reason for the 2017 revision, because recently the discussion about "compliance" and "business ethics" became increasingly important[4]. The changes start already in the foreword, where general principles of the Code are laid down. After the statement, that the Code highlights the obligation of the Management and Supervisory Boards to ensure the continued existence of the company and its sustainable value creation in line with the principles of social market economy (the company's best interest), the following sentences were added:

"These principles not only require compliance with the law, but also ethically sound and responsible behavior (the "reputable businessperson" concept, *Leitbild des Ehrbaren Kaufmanns*).

Institutional investors are of particular importance to companies. They are expected to exercise their ownership rights actively and responsibly, in

3) Published in the Federal Gazette (BGBl) 24 April 2017.

4) One example is the recently established EU General Data Protection Regulation (GDPR) of April 27, 2016, enforced EU-wide on May 25, 2018.

accordance with transparent principles that also respect the concept of sustainability."

In order to understand, what is meant by a "reputable businessperson", one might be reminded in Japan of the traditional merchant, concentrating his activities mainly on a long term relationship with customers rather than short term profit, and relying on the "*giri-ninjo*" principle as an important factor in social and business relationship. But whereas it seems, that there is no direct translation in Japanese, which reflects/expresses the same idea behind it, this notion of "reputable businessperson" has a long history in Europe/Germany and is still nowadays used as a legal term[5]. Its history goes back as far as the 12th century, when the ideal of a "reputable businessperson" was taught in medieval Italy and in the Hanseatic League in the 14th century in Northern Germany.

In Germany, the "*Ehrbarer Kaufmann*" is a model concept of an optimal acting economic subject and this ideal is expressed also in the law: §1 of the above mentioned German IHK-Law says clearly, that "The Chambers of Commerce have to support and consult…, and have to look after the protection of integrity and morals of the reputable businessperson."

Consequently, this is relevant for anyone, taking part in business activities, including managers, merchants, entrepreneurs or people doing one-man-business.

Although there are a lot of synonymous expressions in this context, they are all based on a common, historically developed idea, which has, nevertheless, to be considered always in the context of its time.

---

5) Law regulating legal issues of the Chambers for Commerce and Industry (IHK-law, Gesetz zur vorläufigen Regelung des Rechts der Industrie- und Handelskammern) from 18.12.1956 (BGBl. I, S. 920), last change on 29.3.2017; BGBl. I S. 626).

If we talk about “ehrbar” in German or “reputable” in English, we have already two notions, which do not necessarily mean the same with respect to its cultural context: The German word stresses more the concept of “honour”, a word, which is strongly related to the value system in a respective society. In Germany, this system is on one side influenced by Christian religion, on the other by a humanistic education, based on the ideas of the area of enlightenment.

It would be interesting, to go deeper into the various concepts of the “reputable businessperson”, but it would lead us too far away from the subject of this paper. Anyhow, this short excursion shows, how traditional concepts still influence todays legal regulations.

1.2.2 The Compliance Management System (CMS) and Whistleblowing System

1.2.2.1 CMS

Another important change took place with regard to the tasks of the Management Board, which are regulated in Section 4 of the GCGC. In Para. 4.1.3 it said up to now only, that “the Management Board ensures that all provisions of law and the company’s internal policies are complied with, and endeavors to achieve their compliance by the group entities (Compliance).” So this in itself can be regarded as a soft-law definition of “Compliance”, but it proved to be too general in content without any instruction, how this kind of compliance should be put into practice. As a consequence, with the reform of 2017 it was introduced a kind of guideline or manual, how this aim should be achieved and the following sentences were added:

“It shall also institute appropriate measures reflecting the company’s risk situation (Compliance Management System) and disclose the main features

of those measures. Employees shall be given the opportunity to report, in a protected manner, suspected breaches of the law within the company; third parties should also be given this opportunity."

The reform thus provides two kind of measures in order to enforce compliance with the provisions of law and the company's internal policies:

a) The Management Board shall establish a compliance Management System, and

b) A system for employees and third parties, to report "in a protected manner" about breaches of law, which is nothing else than a whistleblower system.

Although the introduction of a compliance management system is part of the "comply or explain" regulation of the code, it is already widely accepted in company practice and it is worthwhile to look at some examples, how this system has been implemented so far. A practical and representative example for the importance of compliance is, that the biggest private bank in Germany, Deutsche Bank, recently made public, that it will increase its department "Compliance, Regulation and Combat against financial crime" by further 400 people, from now 2600 to 3000 at the end of the year[6]. In addition, the following statement on the bank's homepage makes clear the awareness of a "compliance consciousness" in companies and describes in more detail, how a compliance system should be managed adequately:[7]

"In our view, responsible corporate governance does not only mean adherence to laws, regulations, and standards. It requires a stringent compliance system. We have defined strict rules and guidelines for our

6) https://www.wr.de/wirtschaft/deutsche-bank-400-neue-mitarbeiter-fuer-compliance-abteilung-id214068305.html; see also general statement and detailed compliance examples: https://www.db.com/cr/en/concrete-compliance.htm;

7) https://www.db.com/cr/en/concrete-compliance.htm

staff across the entire spectrum of our areas of activity. Through our conformity with the law, we ensure that the company, its shareholders, clients and employees are protected as comprehensively as possible.

We expect all of the employees of Deutsche Bank to adhere to our compliance standards – by conducting themselves honestly, responsibly and ethically. Our Code of Ethics describes the values and standards for ethical business conduct and serves as the guiding principle for all of our interactions – regardless of whether they are with clients, competitors, business partners, government and regulatory authorities, shareholders or among one another. At the same time, it forms the foundation of our compliance principles, which provide our staff with precise guidelines for proper behavior. That is how we strive to ensure conformity with all applicable laws, regulations and standards.

In order to promote our responsible behavior on the part of our staff, we have expanded our mandatory training on compliance issues. Failure to complete mandatory compliance trainings now carries clear consequences, for example in regard to compensation.

Furthermore, to support our controls systems we have substantially expanded our "Red Flag" monitoring system. It reports all violations of compliance requirements in specific areas."

The compliance department in this company is independent of the operational business of the bank. As in other areas of corporate governance, this system can work only, if the institution, which should control another within an organizational entity (like control of management board by supervisory board) is independent enough, and it seems to be an eternal discussion, whether we can talk about "real" or only formal independence.

The Deutsche Bank tries to give prove of the compliance department, by describing its competences:

"Using our Compliance Control Framework as a basis, we are raising the level of awareness of conformity with the law in our operational business areas. The framework specifies the functions of the Compliance team in detail.

The team is responsible for:

- *providing advice to individual business units on applicable laws, directives, standards, and regulations as well as providing compliance support*
- *monitoring trades, transactions and business processes in order to identify any potential compliance risk*
- *developing globally or locally applicable principles, standards and guidelines for Compliance, communicating them and verifying adherence*
- *maintaining the Bank's internal watch and restricted lists of projects to which special attention must be paid*
- *helping to achieve adherence to the Bank's internal confidentiality regulations ('Chinese walls')*
- *implementing any measures arising from the anti-money laundering program*
- *ensuring that any occurrences which give reason to suspect money laundering or the financing of terrorism are identified and reported to law enforcement authorities*
- *providing regular training and education for staff on the applicable regulations, rules and internal standards*
- *coordinating risk control and monitoring the management of reputational risk*

- *communicating with regulatory agencies around the world on a daily basis."*

Although there are some areas of business, which are specific for banks, most of the indicated measures could be implemented also in other business areas.

Interesting in this context is the so called "Red Flag system", which is used to get control over employees' behavior. It uses objective measures to assess employees' adherence to risk-related policies and processes, allows senior managers to address risks more effectively and creates a stronger link between behavior and reward.

Employees in breach of an applicable policy or process receive a Red Flag. All Red Flags are risk-weighted depending on the severity and frequency of the incident. Aggregated Red Flag scores are taken into account in reviews of performance, pay and promotion.

Since the introduction of Red Flags, the number of breaches has decreased steadily, indicating a positive change in risk-related behaviors.

Finally, within this context, any compliance management system has to take into account and enact, especially with regard to the below mentioned new regulation concerning data protection, effective policies, rules, standards and processes, which apply to data protection in day-to-day operations[8]. They have to ensure compliance with all relevant statutory regulations, which may vary considerably from one country to another.

This question is therefore especially important for globally acting

8) https://www.db.com/cr/en/concrete-compliance.htm

companies, but independent of the various business cultures and standards, which might apply in the respective head offices/home countries, everybody must be aware, that companies always have to adapt to the (compliance) rules in the country or area of business activity. This is now especially important f.i. for Japanese companies doing business in the EU. The recently enforced EU-law [General Data Protecion Regulation (GDPR)] on Data protection is of highest relevance and its practical and legal relevance cannot be underestimated (more details in Chapter II).

1.2.2.2 Whistleblowing System

a) Since the introduction of the U.S. Sarbanes-Oxley Act in 2002 and several other national corporate governance codes, whistleblowing policies have been implemented in a growing number of companies. Existing research indicates that these types of governance codes have a limited direct effect on ethical or whistleblowing behavior, whereas whistleblowing policies at the corporate level seem to be more effective. Therefore, evidence on the impact of (inter-) national corporate governance codes on the content of corporate whistleblowing policies is important to understand their indirect impact on whistleblowing behavior.

Para. 4.1.3 sentence 3 GCGC now stipulates, as mentioned above, the establishment of a whistleblower system:

‚Employees shall be granted the opportunity to report statutory violations in a secure and proper way.‘

This provision for the first time includes the recommendation to set up a protected information system (whistleblower system) for employees. Most

companies already have a more or less substantial CMS. However, numerous companies forego the establishment of a whistleblower system (also known as ‚*Whistle-Blower-Hotline*') so far, as it leads to further data protection, labor law and organizational implications (e.g. IT infrastructure). Moreover, anonymous hints need to be investigated, which in turn implicates further effort. Even though the explicit recommendation for a whistleblower system may be very surprising, it is reasonable enough nowadays, because only an active compliance organization (this includes a whistleblower system) may result in avoidance of liability (monetary fines due to compliance violations are in most cases based on sec. 30, 130 OWiG (Administrative offences Act) or sec. 81 GWB (Act against restraint of competition))[9].

b) Establishment of a whistleblower system for third parties

Further, the GCGC also suggests the establishment of a whistleblower system for third parties. According to the Code's expectation, third parties shall also be granted the opportunity to report irregular practices or suspected cases. As this is only a suggestion ('should'), there is no need to execute a compliance or non-conformance statement according to sec. 161 subsection 1 AktG (Stock Corporation Act) if such system is not introduced. Nevertheless, the extension of the system to third parties can also be understood as the intention of the law makers, to use all possible means in order to uncover irregularities within a company or group of companies (Konzern) and make company leaders aware and let them pay even more attention to the compliance system. It also offers the opportunity for employees, who are afraid of acting as whistleblowers by themselves, to give information to a third party, which may then take over the role of an

9) https://www.deloitte-tax-news.de/german-tax-legal-news/new-revision-of-the-german-corporate-governance-code-increased-demands-on-compliance-management-systems.html

“instructed whistleblower”.

1.2.3 Reform of tasks of the Supervisory Board

a) Investors vs shareholders

Besides some minor statutory changes with regard to remuneration in 4.2.3, the third significant reform concerns various tasks and activities of the Supervisory Board. First, Para. 5.2 says, that the Chairman of the Supervisory Board should be available – within reasonable limits – “to discuss Supervisory Board-related issues with investors”. The code does not talk in this context about “shareholders” in general, although any shareholder can be looked at as an investor. In practice, it is in principle clear, that an investor is meant to be a shareholder with a higher investment than average. But the law remains vague and offers neither a definition of “investor”, nor makes it clear, what Supervisory Board-related issues should be. So, the question is in fact, why this regulation had been introduced and for what purpose.

One possible explanation might be, that it is apt to promote more transparency and eventually to prevent insider trade problems. If we look at the tasks of the Supervisory Board, as described in 5.1.1, it is about advising and supervising the Management Board in its management of the company, and it must be involved in all decisions of fundamental importance of the company. And of course, it is at the discretion of the Chairman, if and to what extent he will make himself available for discussion with investors. And as the code says “should”, this regulation is also not part of the “comply or explain-rule”, so it is not necessary to give any statement on the company’s homepage, if the chairman decides not to discuss with investors. The only reason to follow this recommendation anyway will finally be the consideration of profit for the company: being available for discussion with investors is a so called “trust-building” measure, may lead to stabilize the investment situation

and make shares even more attractive and valuable.

b) Year-end-audit and selections of external auditors (public accountant)

If an Audit Committee is established within the Supervisory Board, its tasks has been now enlarged to monitor not only the accounting process, but the accounting itself, and newly introduced is the obligation, to submit to the Supervisory Board a reasoned recommendation for the appointment of an (external) auditor in order to establish and publish the Year-end report on accounting (5.3.2). The reason behind this new regulation is, to further strengthen the independence of the companies' audit, always having in mind the various, especially financial scandals, in which major companies, not only or necessarily German companies, have been involved in the past. It is also a sign, that on one side legal regulations are often behind economic practice, which presents – intentionally or not – always new scenarios, which lead to damages of companies or even to economic crisis. In this context, the external audit plays an extremely important role to insure the creditability of the figures, which are the basis for investors decisions.

On the other hand, the law had to find also a practical solution, which resulted in the following:

The reasoned recommendation, which the Audit Committee has to submit to the Supervisory Board, should comprise at least two candidates, if the audit engagement is put out to tender. In addition, the Audit Committee has to monitor the auditor's independence and concerns itself with the additional services rendered by the auditor, the issuance of the audit engagement, the determination of the key audit areas and the fee agreement.

Of course, it is easier said than done to monitor "the auditor's

independence" and it is a fact, that the lack of auditor independence is one of the major issues in the recent history of corporate governance.

In this context, it is important to know, that the law provides in Sections 319 and 319a of the German Commercial Code (HGB) some of the criteria, which are relevant to determine the independence of external auditors:

"§ 319 HGB: Selection of Certified Public Accountants (Annual Auditors) and reasons for exclusion

(1) Annual auditors can be certified public accountants (Wirtschaftsprüfer) and German public audit firms (Wirtschaftsprüfungs gesellschaften). Auditors of annual accounts and annual reports of medium-sized companies with limited liability (§ 267 par. 2 HGB) or of medium-sized trading partnership in the sense of § 264a 1 HGB can also be German sworn auditors or German firms of sworn auditors. An annual auditor must have pursuant to sentences 1 and 2 an effective excerpt of the professional register, which proofs that the registration took place in accordance with § 38 no 1 h or no 2 f of the Public Accountant Act (Wirtschaftsprüferordnung, WPO)[10]*. Annual auditors who perform*

10) § 38 Entry

The initial entries in the public register consist of the responsible parties for admission, quality assurance, disciplinary and public oversight according to § 66a (designations, addresses) of all members of the profession and audit firms, followed by individual listings next to the respective registration number

1.Professional Accountants in Public Practice, including

h) Notification of the activity as a statutory auditor according to § 57a Section 1 Sentence 2,

2. Audit firms, including

f) Notification of the activity as a statutory auditor according to § 57a Section 1 Sentence 2.

§ 57a Quality Assurance Review

Sole practitioners and audit firms are obliged to undergo a quality assurance review if they intend to conduct statutory audits according to § 316 HGB. They are required to notify this intention to the Chamber of Public Accountants at the latest two weeks after the acceptance of an audit engagement. Nature and scope of the activity shall be reported with the notification.

for the first time an annual financial statement required by law in accordance with § 316 HGB have to provide an excerpt of the professional register at least six weeks after they accepted the audit assignment. During an ongoing annual audit the accountants have to indicate vis-à-vis the company, if the registration has been deleted.

(2) a public accountant or sworn auditor is excluded as annual auditor if during the business year, for which the annual report to be examined or during the final audit reasons come up, notably concerning business-related, financial or personal relations, which rise concerns of partiality.

(3) a public accountant or certified public accountant is excluded in particular from the final exam if he or a person with whom he jointly exercises his profession,

1. owns shares or has other major financial interests in the Corporation to be audited, or a stake in a company, which is connected with the Corporation to be audited or owns from that company more than twenty per cent of the shares.

2. is a legal representative, Member of the Supervisory Board or employee of the Corporation to be audited or of a company, that is connected with the Corporation to be audited or owns from that company more than twenty per cent of the shares;

3. has beyond the audit work at or for the Corporation to be audited during the audit-business year or until the issuance of the audit

Significant changes to the nature and scope of the audit work shall also be reported.

certificate

a) participated in the bookkeeping or the preparation of annual financial statement,

b) participated in the implementation of the internal audit in a responsible position,

c) provided management or financial services

d) provided insurance-mathematical or evaluation services, which have not only marginal effect on the to be audited annual statement provided that these activities are of minor importance; the same applies if one of these activities is performed by an enterprise for the corporation to be audited, in which the accountant or sworn auditor is legal representative, employee, member of the Supervisory Board or a shareholder, who owns more than twenty per cent of the shareholders admitted voting rights;

4. employs a person at the audit, who is not admitted as auditor according no. 1 to 3;

5. has received during the previous five years respectively more than thirty per cent of the total revenue of his professional activities from one of the of the Corporation to be audited and from companies, where the Corporation to be audited owns more than twenty per cent of the shares, and the same is expected for the current business year; in order to avoid hardship the Chamber of Public accountants may grant temporary exemptions.

This also applies if the spouse or life partner fulfills one of the grounds of exclusion mentioned in sentence1 No. 1, 2, or 3.

(4) audit corporations and book auditing companies are excluded from the audit, if they themselves, one of their legal representatives, a shareholder who owns more than twenty per cent of the shareholders voting rights, an affiliated company, a shareholder employed during the audit in a responsible position or another employed person, may affect the result of the audit, are excluded according to paragraph 2 or paragraph 3. Sentence 1 shall also apply if a member of the Supervisory Board is excluded according to paragraph 3 sentence 1 No. 2, or if several shareholders who own together more than twenty per cent of the voting rights, are individually or together excluded according to paragraph 2 or paragraph 3.

(5) Paragraph 1 sentence 3 and paragraphs 2 to 4 shall be applied respectively to the auditor of the consolidated financial statement."

"§ 319a HGB: Special grounds for exemption for companies of public interest

(1) A certified public accountant (Wirtschaftsprüfer) is besides the grounds referred to in § 319, paragraph 2 and 3, excluded from auditing a company which is capital market-oriented in the sense of § 264d, is a CRR-credit institution in the sense of section 1paragraph 3d sentence 1 of the Credit System Law, with exception of the institutes mentioned in section 2 paragraph 1 no.1 and 2 of the Credit System Law, or is an insurance company in the sense of article 2 paragraph 1 of the Directive 91/674EWG

also if he

1. (abolished)

2. has provided during the business year for which the annual financial statement should be established tax advisory services in the sense of section 5 paragraph 1 sub-paragraph 2 a (i) and (iv to vii) of the Regulation (EU) No. 537/2017, which have individually or together direct and not only unessential effect on the statement to be audited; a not only unessential effect is the case, if the provision of tax advisory services in the business year to be audited has reduced considerably the domestic profit to be allocated for tax purposes or if a considerable portion of the profit has been shifted abroad without a mere tax profit exceeding economic necessity for the company was at stake, or

3. has during the business year to be audited or until grant of the audit certificate has provided for the corporation beyond the audit activities evaluation services in the sense of of section 5 paragraph 1 sub-paragraph 2 f of the Regulation (EU) No. 537/2017, which have individually or together direct and not only unessential effect on the statement to be audited.

§ 319, paragraph 3, sentence 1 No. 3 last part of sentence, sentence 2 and paragraph 4 shall apply respectively to the grounds for exclusion referred to in sentence 1. Sentence 1 no.2 and 3 will also apply, if persons, with whom the public accountant practices his profession fulfill the grounds for exclusion mentioned there; if the public accountant provides tax advisory services in the sense of section 5 paragraph 1 sub-paragraph 2 a (i) and (iv to vii) of the Regulation (EU) No. 537/2017 or evaluation services in the sense of section 5 paragraph 1 sub-paragraph 2 f of the Regulation (EU) No. 537/2017, he has to describe and explain the effect of these activities on the performance of the audit. Responsible partner of the audit is the person who signs the audit certificate according to § 322

or the person who is nominated by an audit corporation as responsible auditor for the performance of the audit.

(1a) By application of the auditor the regulatory authority for auditors at the Federal Office for Economy and Export Control may exempt him exceptionally for maximum one business year from the requirements of Article 4 paragraph 2 subparagraph 1 of the Regulation (EU) No. 537/2017, but only up to 140 percent of the average remuneration mentioned in Article 4 paragraph 2 subparagraph 1 of the Regulation (EU) No. 537/2017.

(2) paragraph 1 shall apply respectively to the auditor of the consolidated financial statements. As responsible audit partner at group level is considered also the person, who has been designed as an auditor at the level of major subsidiaries as for performing their audit in a primarily responsible position.

(3) The audit committee of the company has to approve in advance the provision of tax advisory services in the sense of section 5 paragraph 1 sub-paragraph 2 a (i) and (iv to vii) of the Regulation (EU) No. 537/2017 by the auditor. If the company has not established an audit committee, the Supervisory Board or Board of Directors has to approve.

c) External Monitoring System

Besides the monitoring by the companies audit committees, there exists an additional monitoring system on the quality of the public accountants work and their independence, done by the Chamber of Public accountants (Wirtschaftsprüferkammer, WPK), mentioned also in the law above, which is a kind of professional's representative body and plays an important role in insuring the independence and reliability of the profession of public accountants[11].

The WPK is a corporation under public law, whose members are all (German) public accountants (Wirtschaftsprüfer), German sworn auditors [(vereidigte Buchprüfer (licensed auditors in public practice authorised to perform only statutory audits of annual financial statements of mid-sized German limited liability companies (GmbH))], German public audit firms (Wirtschaftsprüfungsgesellschaften) and German firms of sworn auditors (Buchprüfungsgesellschaften), headquartered in Berlin and competent for its more than 21,000 members throughout Germany.

As the representative of the entire profession of auditors in Germany, WPK represents their professional interests towards the public and articulates these interests towards lawmakers, competent courts and other authorities. WPK is responsible for the appointment of auditors and the recognition of audit firms as well as for their revocation. Appointment and recognition constitute membership with WPK. The organization monitors the compliance of its members with their professional duties (§ 57 para. 1 Public Accountant Act (WPO))[12]. In case of a breach of duties the Management

11) https://www.wpk.de/eng/

12) § 57

Functions of the Chamber of Public Accountants

(1) The Chamber of Public Accountants fulfils its statutory functions; it is to uphold the interests of all of its members and to supervise the fulfilment of the professional duties.

(2) In particular, it is the responsibility of the Chamber of Public Accountants:

1. To advise and instruct the members in questions concerning professional duties,
2. Upon request, to mediate conflicts amongst members,
3. Upon request, to mediate conflicts between members and their clients,
4. To oversee members' compliance with their duties and irrespective of § 66a Section 4 Sentence 2 and Section 6 to impose professional disciplinary measures,
5. (repealed),
6. In all matters pertaining to members collectively, to bring forth the views of the Chamber of Public Accountants vis-à-vis the competent courts, authorities and organizations;
7. To submit expert opinions as requested by a court or an administrative agency or an entity involved in the legislation at national or state level,

Board of WPK is responsible for sanctioning this breach (§ 68 WPO). Possible disciplinary measures are reprimands, fines up to 500.000 EUROs, temporary prohibition from certain types of professional activities or final exclusion from the profession. In case of a repeated occurrence of breaches, WPK may also declare a prohibition order. Breaches of professional duties related to statutory audits of public interest entities according to § 319a para. 1 HGB are within the responsibility of the Auditor Oversight Body (AOB), which is established at the Federal Office for Economic Affairs and Export Control (BAFA).

Members may raise objections to disciplinary measures. Subsequent to a fully or partially unsuccessful objection dealt with by the Board of Management of WPK a member may appeal for a professional court proceeding. The so-called professional courts (special divisions of criminal courts/Senate at the District Court of Berlin in the First Instance, Superior Court of Justice of Berlin in the Second Instance and the Federal Court of Justice in the Third Instance) are responsible in these cases. The

---

8. To assume the tasks in the areas assigned to it by law in the field of occupational training;
9. (repealed),
10. To promote the continuing professional development of the members and the initial professional development of future members of the profession,
11. To submit proposals for honorary associate judges of the disciplinary courts to the State Departments of Justice and the Federal Ministry of Justice,
12. To maintain the public register,
13. To establish pension schemes for Professional Accountants in Public Practice and Sworn Auditors and their surviving dependents,
14. To maintain a quality assurance system,
15. To appoint Professional Accountants in Public Practice as well as Sworn Auditors, to license audit firms and firms of Sworn Auditors and to withdraw or revoke licensing,
16. To create and maintain an independent Examination Unit,
17. To carry out the statutory responsibilities conferred upon it as a professional chamber within the scope of the prevention of money laundering.

professional courts are assisted by members of the profession who bring in their professional expertise. WPK continuously reviews annual and consolidated financial statements audited by its members and published in the Federal Gazette on a random basis. Objective of the financial statement review is to verify whether the published financial statements and the corresponding auditor's opinions comply with legal and professional requirements. However, financial statements of public interest entities according to § 319a para. 1 HGB are not covered by this review. These companies are subject to the direct public oversight of AOB.

Furthermore, it exists a multi-layer quality assurance system, which is intended to ensure that the quality control systems of the professional practices are subject to a regular, preventive monitoring process (quality assurance reviews). Auditors, to the extent they conduct statutory audits according to § 316 HGB, must have their practice monitored by an independent auditor ("peer") for quality assurance every six years. If a practice performs statutory audits as defined in § 316 HGB for the first time, it shall undergo a quality assurance review not later than three years after the beginning of the first audit. The quality assurance review comprises an evaluation of the internal quality control system of each practice, which is evaluated in terms of its appropriateness and ability to function. This pertains particularly to compliance with the professional requirements (WPO, Professional Charter and other professional regulations), independence requirements, quality and quantity of the resources deployed as well as the remuneration charged.

Within WPK the Commission on Quality Assurance is responsible for the quality assurance system. The Commission decides about measures aimed at

remedying deficiencies. It is furthermore responsible for the registration of quality assurance reviewers and may reject reviewers proposed by an audit firm. The Commission exercises the oversight on the quality assurance reviewers and may participate in the performance of a quality assurance review. The Commission on Quality Assurance issues annual reports on its activities.

The Auditor Oversight Body (AOB) at the Federal Office for Economic Affairs and Export Control (BAFA) monitors if the quality assurance procedures of WPK are performed on an appropriate, adequate and proportionate basis. The ultimate decision making power about rulings of the Commission on Quality Assurance lies with AOB.

The evaluation of the internal quality control system of audit firms that also conduct statutory audits of public interest entities (§ 319a para. 1 HGB) is performed by AOB through inspections – as far as the public interest entities are affected.

In summary, it can be said, that the control-system of public accountants, who finally have to certify the correctness of data and information presented by companies in public and which are the basis of for financial investment, has developed in Germany to a highly reliable standard.

d) Composition of the Supervisory Board

Critical voices in recent years about the performance and competence of the Supervisory Board, whose main task is, according to §111 AktG (German Stock Companies Act), "to monitor the Management" of the company, has led to a revision of Section 5.4 of the GCGC, which deals with the composition of the Supervisory Board: The composition of the SB should ensure that its members collectively have the knowledge, skills, and

professional expertise required to properly perform all duties. The critics were especially loud during the bank crisis, which led in 2010 to drastic measures by the Federal Financial Supervisory Authority (BaFin)[13] : it cancelled the nomination of several, newly nominated members of Supervisory Boards in the financial sector, due to incompetence. This special control power had been transferred to BaFin by a new law, established as an answer to the Lehman-Shock.

SB incompetence is not only a problem in the private sector: there are also large deficiencies in public projects like the new International Airport in Berlin. Due to the incompetence in the Supervisory Board, where also politicians have a seat, since years an endless amount of money is burned every day without remarkable progress.

The GCGC now provides the duty for the SB to prepare a profile of skills and expertise for the entire Board. Especially new is, that the specific requirements of the co-determination act (Mitbestimmungsgesetz) have to be taken into account in regard of the elected employee representatives. It is quite interesting to see, that this issue, which concerns a specialty in German Labour and Company Law with already a long history, has to be mentioned now explicitly in the GCGC. It reflects the obvious deficits in the co-determination system on the SB-level.

Not quite new but supplied with a new time-limit is the requirement to increase the share of women in the SB. The GCGC says in 5.4.1, that in listed corporations subject to the Co-determination Act etc., "the Supervisory Board comprises at least 30 % women and at least 30% men (the latter is mentioned just to comply with gender policy…). With effect from 1 January 2016, the minimum share of 30 percent respectively for men and women

13) https://www.bafin.de/EN/Homepage/homepage_node.html

members of the SB must be observed in any new elections or delegations that become necessary for filling individual or several positions in a SB. Consequently, it does not apply to the already and continuously serving members. Nevertheless, a recent research done by the renowned Management consulting firm Kienbaum shows, that "Gender Diversity" is still very low in Germany's 30 Stock-Exchange listed companies.

In order to make competence a transparent factor, it is now required, that the proposal for a SB candidate shall be accompanied by a curriculum vitae, providing information on the candidate's relevant knowledge, skills and experience; it shall be supplemented by an overview of the candidate's material activities in addition to the SB mandate, and shall be updated annually for all SB members and published on the company's website.

2. New regulation on Data protection: The new EU legal setting for data protection

Data protection has become an increasingly important issue in recent years and as a result of the globalization of trade and markets, this issue is no longer a problem restricted to one nation state. The European Union has, after many years of discussion and partial effective legal measures[14] decided

14) After the OECD had tried in 1980 to create a comprehensive data protection system, by issuing the „Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data", and one year later the Council of Europe had negotiated the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data", the fact, that both initiatives had no real binding effect and interpretation of content varied from country to country, the EU introduced in 1995 the EU Data Protection Directive ("Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data"). As a tool for the harmonization of EU law, directives are the most commonly used instrument, but as data flow beyond boarders and through the internet worldwide, it soon became clear, that leaving too much space for

to set up a general framework for data protection, which has its effects not only within the EU and its member states, but can also be effective far beyond its borders. It is therefore of utmost importance also for companies from non-EU countries, which have trade-relations with EU member-states (f.i. Japan), to have some basic knowledge of the new legal setting, and it may also be of some impact for academic scholars from abroad, to participate in the discussion and eventually get some new ideas or awareness for data protection in his or her own country. Within the EU there are various legal instruments to regulate policy related issues, the most important ones are directives and regulations (Art. 282 TFEU).

A "directive" is a legislative act that sets out a goal that all EU member states must achieve. However, it is up to the individual member states to devise their own laws on how to reach these goals. One example is the EU consumer rights directive, which strengthens rights for consumers across the EU, for example by eliminating hidden charges and costs on the internet, and extending the period under which consumers can withdraw from a sales contract, but the way, how this goal will be achieved, is decided by the national parliaments.

A "regulation" is a binding legislative act, immediately effective in all member states after its release. It must be applied in its entirety across the EU. For example, when the EU wanted to make sure that there are common safeguards on goods imported from outside the EU, the Council adopted a regulation.

---

implementation of the directive through national law will not meet the requirements of an effective data protection system. The Directive was finally amended by Regulation No. 1882/2003 and now replaced by the GDPR.

2.1 *The Data Protection Law Enforcement Directive*

The Directive (EU) 2016/680 concerns the protection of natural persons regarding processing of personal data connected with criminal offences or the execution of criminal penalties, and on the free movement of such data. The directive protects citizens' fundamental right to data protection whenever personal data is used by criminal law enforcement authorities for law enforcement purposes. It will in particular ensure that the personal data of victims, witnesses, and suspects of crime are duly protected and will facilitate cross-border cooperation in the fight against crime and terrorism. The directive entered into force on 5 May 2016 and EU member states had to transpose it into their national law by 6 May 2018.

2.2 *The EU General Data Protecion Regulation (GDPR)*

2.2.1 General

Compared to the above-mentioned Directive, the Regulation (EU) 2016/679 (GDPR) is of much broader effect and importance. It is aimed to protect all EU citizens with regard to the processing of personal data and on the free movement of such data and has been recognized as an essential step to strengthen individuals' fundamental rights in the digital age and facilitate business by clarifying rules for companies and public bodies in the digital single market. In addition, the positive effect of the GDPR is, that it eliminates the current fragmentation in different national systems and unnecessary administrative burdens. It entered into force on 24 May 2016 and applies since 25 May 2018.

2.2.2 Extraterritorial Applicability

The biggest change to the regulatory landscape of data privacy comes with

the extended jurisdiction of the GDPR, as it applies to all companies processing the personal data of data subjects residing in the Union, regardless of the company's location. Previously, territorial applicability of the directive was ambiguous and referred to data process 'in context of an establishment'. This topic has arisen in a number of high profile court cases. GDPR makes its applicability very clear: it applies to the processing of personal data by controllers and processors in the EU, regardless of whether the processing takes place in the EU or not.

The GDPR also applies to the processing of personal data of data subjects in the EU by a controller or processor not established in the EU (f.i. Japan), where the activities relate to: offering goods or services to EU citizens (irrespective of whether payment is required) and the monitoring of behavior that takes place within the EU. Non-EU businesses processing the data of EU citizens also have to appoint a representative in the EU.

2.2.3 Practical aspects

In order to understand the complexity and practical importance of the new law, its main content can be summarized as follows:[15)]

The GDPR is mainly focused around consent, legitimate use and other aspects of data protection. Although data security occupies little of the text it does have big significance with new stricter, more specific, obligations on both data processors and controllers. There are no specific controls but instead both controllers and processors are required to "implement appropriate technical and organizational measures" (Art. 24 Para.1 GDPR).

15) It is also highly recommended to read first the legal Definitions, which the law provides in Art.4. In altogether 26 paragraphes, the law explains fi what is meant by personal data", processing, psoydominsation etc. The whole legal text must be read and understood on the basis of these legal definitions.

This is qualified by referencing "the state of the art and the costs of implementation" (preliminary note 78, 83; Art. 25 Para. 1, 32 Para.1 GDPR) and "the nature, scope, context, and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons" (preliminary note 74, 76, 90; Art. 25 Para. 1, 32 Para.1, 35 Para.1, 39 Para.2 GDPR).

Although some of these issues are already covered by existing data protection laws, the GDPR goes further and suggests what kinds of security controls might be considered "appropriate to the risk," including:

• The pseudonymisation (this can be viewed as "reversible" anonymisation) and encryption of personal data.

• The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.

• The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.

• A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing (preliminary note 26, 28, 29, 75, 85, 156; Art. 4 Para. 5, 6 Para.4 d, Art. 25 Para 1, 32 Para.1 a-d, 40 Para. 2 d, 89 Para. 1, GDPR).

To demonstrate compliance with the GDPR the controller or processor should "maintain records of processing activities" (preliminary note 82 GDPR). Precondition to control Personally Identifiable Information (PII) within an organization/company, the locations and systems where PII might be found have to be discovered and documented first. In most organizations collections of "dark data" exist, which are data hidden from the known or formal infrastructure – these databases can vary from small data stores on

individual user's PC's through to large database applications which are not being managed as part of the core infrastructure – and may leak outside of the organization into third parties. Technologies exist to locate and document where PII might exist. These are typically called "Data Discovery" tools – some of which are configured to find particularly sensitive types of data such as credit-card numbers, racial terms, personal identifiers and data patterns. These tools could search through an entire connected infrastructure – networks, PC's servers and even mobile devices and catalogue all the data discovered. Importantly this can be a basis for a "PII Data Asset Register" which will become a vital asset to meet any form of Data compliance.

2.2.4 Penalties

Organizations in breach of GDPR can be fined up to 4% of annual global turnover or €20 Million (whichever is greater). This is the maximum fine that can be imposed for the most serious infringements e.g. not having sufficient customer consent to process data or violating the core of Privacy by Design concepts (Art. 83, 84 GDPR). There is a tiered approach to fines e.g. a company can be fined 2% for not having their records in order (Art. 28 GDPR), not notifying the supervising authority and data subject about a breach or not conducting impact assessment. It is important to note that these rules apply to both controllers and processors – meaning 'clouds' are not exempt from GDPR enforcement.

2.2.5 Consent as Precondition

The conditions for consent have been strengthened, and companies are no longer able to use long illegible terms and conditions full of legalese. The request for consent must be given in an intelligible and easily accessible form, with the purpose for data processing attached to that consent. Consent

must be clear and distinguishable from other matters and provided in an intelligible and easily accessible form, using clear and plain language. And it must be as easy to withdraw a consent as it is to give it (Preliminary note 32 GDPR).

2.2.6 Data subject rights

Under the GDPR, breach notifications are now mandatory in all member states where a data breach is likely to "result in a risk for the rights and freedoms of individuals" (Preliminary notes 83, 85; Art. 27 Para.2 a, 30 Para. 5, 33 Para.1 GDPR). This must be done within 72 hours of first having become aware of the breach. Data processors are also required to notify their customers, the controllers, "without undue delay" after first becoming aware of a data breach.

Part of the expanded rights of data subjects outlined by the GDPR is the right for data subjects to obtain confirmation from the data controller as to whether or not personal data concerning them is being processed, where and for what purpose. Further, the controller shall provide a copy of the personal data, free of charge, in an electronic format. This change is a dramatic shift to data transparency and empowerment of data subjects.

Also known as Data Erasure, the right to be forgotten (preliminary note 65 GDPR) entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data. The conditions for erasure, as outlined in Art. 17 GDPR, include the data no longer being relevant to original purposes for processing, or a data subject withdrawing consent. It should also be noted that this right requires controllers to compare the subjects' rights to "the public interest in the availability of the data" when

considering such requests (preliminary notes 68, 69, 122, 128, 142, 156; Art. 6 GDPR).

Privacy by design as a concept has existed for years, but it is only just now becoming part of a legal requirement with the GDPR. At its core, privacy by design calls for the inclusion of data protection from the onset of the designing of systems, rather than an addition. More specifically, 'The controller shall… implement appropriate technical and organizational measures… in an effective way… in order to meet the requirements of this Regulation and protect the rights of data subjects'. Article 23 calls for controllers to hold and process only the data absolutely necessary for the completion of its duties (data minimization), as well as limiting the access to personal data to those needing to act out the processing.

2.2.7 Local Data Protection Agency

Under GDPR it is not necessary to submit notifications / registrations to each local DPA of data processing activities, nor is it a requirement to notify / obtain approval for transfers based on the Model Contract Clauses (MCCs). Instead, there are internal record keeping requirements, as further explained below, and DPO appointment is mandatory only for those controllers and processors whose core activities consist of processing operations which require regular and systematic monitoring of data subjects on a large scale or of special categories of data or data relating to criminal convictions and offences.

Importantly, Data Protection Officers

- Must be appointed on the basis of professional qualities and, in particular, expert knowledge on data protection law and practices
- May be a staff member or an external service provider

• Contact details must be provided to the relevant DPA

• Must be provided with appropriate resources to carry out their tasks and maintain their expert knowledge

• Must report directly to the highest level of management

• Must not carry out any other tasks that could results in a conflict of interest.

3. Summary

The reform of the German Corporate Governance Code in 2017 has brought a variety of new tasks to the Management and Supervisory Boards, reflected especially in the area of compliance, which has become a new area of legal expertise and for sure will create a new job-category (Compliance Management) as well as increasing mandates for professional lawyers and law firms. Compliance has become especially important with regard to the enactment of the EU General Data Protection Regulation (GDPR), the importance of which has become aware only gradually in companies, not only within the EU, but also outside - as far as they have trading relations with the EU. Independent from business activities, data protection has developed to be a more and more a central issue in business activities and the seriousness of this issue is to some extent reflected with the penalties, which might be charged to companies, who do not comply with the new law – as manifold mentioned independent if the headquarter is within or outside the EU.[16)]

16) The importance of GDPR is also reflected to some extent by the increasing number of publications on this subject, out of which only some examples can be presented here: Jan Philipp Albrecht. How the GDPR Will Change the World. European Data Protection Law Review EDPL, pages 287{289, June 2018; Colin Tankard. What the GDPR means for businesses. Network

Finally, a further special issue to be considered in this context is related to the "historical event" that the UK will leave the EU (Brexit) and almost nobody knows exactly how legal rules will apply after the Brexit[17].

Unlike directives, EU regulations (such as the GDPR) don't have to go through the standard process to become national law. Instead, they become active immediately, meaning that the UK has to follow the GDPR rules until at least the end of March 2019 (based on the expected negotiation timeline).

This is significant as the GDPR itself sets a very high standard for data protection and will have significant effects on UK law during this time. Firstly, the GDPR itself has a wider application, meaning that all companies in all EU nations are now responsible for any data which they process. And processing data can be anything as simple as entering information on a website or social media account[18].

In addition, due to the extraterritorial reach of the GDPR, UK companies continuing to do business with the EU after Brexit will need to comply with the Regulation to avoid infringements. During the referendum campaign in 2016, the Brexiteers consciously supported the false image, that leaving the EU will cut off the relationship also in a legal sense and EU law will no longer be applicable. The GDPR is only one, but a most important example, that this is not the case and makes obvious, that many of the British people had been misinformed about and deceived on the legal effects of the Brexit.

Security, 2016 (6):5 {8, June 2016; Christina Tikkinen-Piri, Anna Rohunen, and Jouni Markkula. EU General Data Protection Regulation: Changes and implications for personal data collecting companies. Computer Law & Security Review: The International Journal of Technology Law and Practice, 34 (1):134 {153, February 2018; Marc Cornock. General Data Protection Regulation (GDPR) and implications for research. Maturitas, 111:A1 {A2, May 2018; EU General Data Protection Regulation (GDPR): An Implementation and Compliance. IT Guidance Publishing, 2017; EU general data protection regulation (GDPR): an implementation and compliance guide. IT Governance Privacy Team, 2016.

17) Which should have become effective on 29 March, 2019; but due to political uncertainties final date is not yet clear at the time of publication of the present article.

18) https://privacytrust.com/gdpr/gdpr-and-brexit.html