MANAGING SUPPLY CHAIN RISK

A legal and strategic perspective

White Paper

June 2021

BOSTON CONSULTING GROUP

CMS law·tax·future

INTRODUCTION

The protection of human rights and the environment is becoming an increasingly important element of the public discourse on sustainability and ESG (Environmental, Social, Governance).

Moreover, corporate social responsibility is no longer regarded merely as a voluntary undertaking. To an escalating extent companies and their management must comply with specific legal obligations ranging from general disclosure to specific risk prevention.

One prominent example is the rapidly evolving legal framework, on a national and European Union (EU) level, for global supply chains. New legislative proposals, such as those from Germany and the EU, introduce specific obligations regarding human rights and environmental due diligence. They compel business entities and their management to implement extended risk analysis tools and preventive measures (such as on-site audits) as well as remedial efforts so that they can confront potential human rights or environmental violations in their supply chains. A failure to conform with these obligations may well result in substantial financial and non-financial risks (including a loss of reputation) for the relevant business entities and their management.

Companies must therefore prepare themselves accordingly. To meet these new legal and risk management obligations and thereby avoid the resulting repercussions, they will need to analyze their value chains carefully. Based on the conclusions reached, they should then optimize their business structures and processes so that they can abide by the new legal standards and meet the expectations of their stakeholders.

As a first step in this process, companies should carefully examine their global value chains and thereby identify their direct and indirect suppliers and other business partners. That should give them a clear picture of their supply chain risks. Depending on the outcome of this risk analysis, companies should then put in place a supply chain compliance program and, most importantly, implement certain tools to select, monitor and control their supply chain partners.

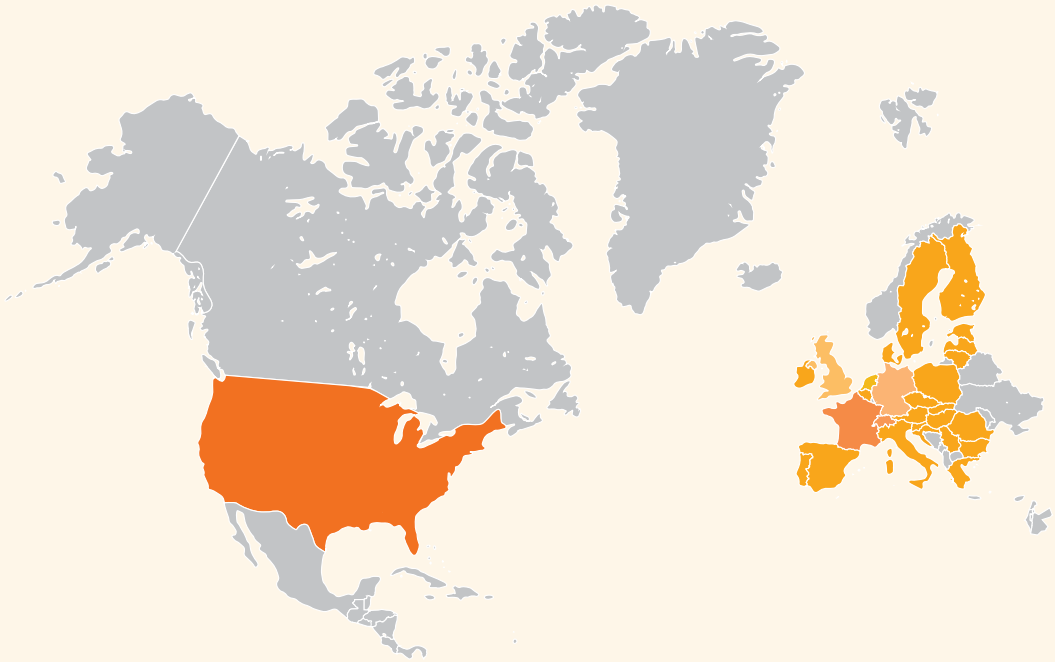
BACKGROUND: Burgeoning legal obligations

During recent years, several national and international laws have established new due diligence obligations for companies regarding their supply chains (See Exhibit 1).

EXHIBIT 1 | International supply chain laws

Growing number of supply chain laws and guidelines establishing new due diligence requirements for companies across the world

Illustrative, non-exhaustive
As of June 2021



US
Section 1502 US Dodd-Frank Act

- Requires US publicly-listed companies to check their supply chains for 3TG and if they originate from the DRC[2] or its neighboring countries
- Passed into legislation in July 2010

EU
Conflict Minerals Regulation

- Compels EU importers of 3TG[1] minerals to meet international responsible sourcing standards; EU member states responsible for enforcement
- In force since January 2021

UK
UK Modern Slavery Act 2015

- Introduces reporting obligations for companies to prevent slavery & human trafficking in their supply chains or own businesses
- In force since accounting year which ends after 31 March 2016

NETHERLANDS
Child Labor Due Diligence Law

- Introduces a duty of care for companies selling goods and services to Dutch end-users to determine whether child labor occurs in their supply chains
- Expected to come into force in 2022, unless replaced by draft law covering human rights in general (currently in parliament)

FRANCE
Corporate Duty of Vigilance Law

- Requires companies to identify risks and to prevent serious harms to human rights and fundamental freedoms, to the health & safety of individuals and to the environment within their global supply chains
- In force since March 2017[3]

SWITZERLAND
KVI[4] Counterproposal[5]

- Mandatory due diligence for conflict minerals and child labor for certain Swiss-based companies[6]
- If enacted, expected to enter into force on 1 January 2022

GERMANY
Supply Chain Act

- Requires companies to check human rights and environmental standards across the entire supply chain
- If enacted, in force from 1 January 2023

1. Tin, tantalum, tungsten and gold ("3TG")
2. Democratic Republic of the Congo
3. Due diligence requirements effective since 28 March 2017, reporting obligations since 1 January 2018
4. Responsible Business Initiative ("Konzernverantwortungsinitiative")
5. In November 2020, the KVI was rejected in a referendum, which paved the way for the less rigorous so-called Counterproposal of the Council of States
6. No due diligence regarding child labor required if undertaking does not reach at least two of the three following criteria: balance sheet total CHF 20M, revenues CHF 40M, 250 FTE

Source: BCG analysis

Laws on human rights and the environment range from reporting obligations to specific due diligence requirements and risk management duties along the entire supply chain. Companies are compelled to monitor, control, and mitigate associated risks, relating for example to child labor, forced labor or to the sourcing of minerals from conflict areas.

Companies with global supply chains, particularly in manufacturing and retail, are now under significant pressure to meet these new requirements. Non-compliance can lead to highly undesirable outcomes for both companies and their leaders. These include severe fines, compensation claims, exclusion from public procurement, and reputational damage among an increasingly aware population of consumers.

Two examples of these legal developments are detailed below:

EXAMPLE 1

Germany's draft proposal for a Supply Chain Act

In 2016, the German government introduced a National Action Plan. It set out expectations to be met by companies by the end of 2020 and introduced a due diligence procedure for safeguarding human rights in their supply chains. The Government initially counted on voluntary participation. However, several monitoring reviews, conducted between 2018 and 2020, revealed that only a small proportion of companies had participated in the program, or put in place any human rights due diligence procedure in their supply chains.

Consequently, in March 2021, the Government published a draft proposal for a German Supply Chain Act. This Act, if passed by parliament, would apply from 2023 to companies (including banks and other financial service providers) with a German headquarter or branch office employing at least 3,000 employees.

The draft proposal is still subject to a controversial discussion. However, if enacted, the German Supply Chain Act will bring in the following mandatory requirements for companies, together with associated state sanctions and powers:

- Establishment of a mandatory risk management system to identify, analyze and control potential human rights and environmental violations in the supply chain
- Introduction of measures to prevent and remediate human rights abuses and environmental violations. These measures include formulating a mission statement, and implementing satisfactory procurement strategies, training and internal controls relating to human rights and the environment
- Introduction of effective remedies in case of human rights abuses and environmental violations
- Implementation of an external complaint mechanism for alleged violations
- Reporting and documentation obligations
- Application of sanctions in case of human rights abuses and environmental violations (including fines and exclusion from public procurement)

EXAMPLE 2

The European Parliament's draft Directive on supply chain due diligence

In March 2021, the European Parliament passed a resolution in which it requested the European Commission to submit a legislative proposal on mandatory supply chain due diligence based on a Draft Directive attached to the resolution. This Directive is intended to apply to large undertakings, to publicly listed small and medium-sized undertakings, as well as to small and medium-sized undertakings operating in high-risk sectors, provided that the said undertakings are established in EU territory, are governed by the law of an EU Member State, or operate in the EU market through the sale of goods or the provision of services. Undertakings include those providing financial products and services.

The EU Draft Directive would bring in the following mandatory requirements, powers and sanctions:

- Introduction of an adequate due diligence procedure regarding human rights, the environment and good governance (including risk analysis, risk prevention and the introduction of a grievance mechanism)
- An obligation to introduce adequate remedial measures and corresponding internal controls
- A duty to publish a strategy on how to approach due diligence requirements relating to human rights, the environment and good governance
- The power of the competent authority to carry out investigations, including interviews and on-the-spot-checks, and in certain severe cases to order the temporary suspension of activities, which, in the case of non-EU companies, may imply the ban on operating in the EU market
- Sanctions, including the imposition of fines and the exclusion of companies from public procurement, and civil liability for human rights violations

The EU Draft Directive is broader than the German legislative proposal in several respects. Its scope of application broadly covers companies doing business in the EU and would therefore have an extra-territorial effect. Furthermore, its application is not limited to companies with a minimum number of employees. Regarding the subject matter, the proposed Directive will not only cover human rights and environmental violations but also good governance (of a country or region), i.e. essentially anti-corruption issues. In contrast to the German proposal (which in its current version primarily focuses on direct suppliers), the proposed EU requirements will apply to the entire supply chain, i.e. any direct or indirect supply chain partner. Finally, the EU Draft Directive provides for civil liability in the event of non-compliance with any of the due diligence obligations (as another sanction in addition to fines and (temporary) exclusion from public procurement); it would need to be transposed into the national law of each EU Member State, and liability will be governed by the Directive as transposed into national law at the place of the court where proceedings are pending.

It should also be noted that, like the planned regulations in Germany and the EU, many other countries have introduced specific ESG requirements. A failure to comply with these legal requirements may also result in significant financial and non-financial risks (including a loss of reputation) for companies and their management (See Exhibit 2).

EXHIBIT 2 | Increased due diligence requirements

Recent legislations significantly increase due diligence obligations for companies with globalized supply chains

Illustrative, non-exhaustive
As of June 2021

Main categories	EU: Conflict Minerals Regulation	GERMANY: Supply Chain Act	FRANCE: Corporate Duty of Vigilance Law	NETHERLANDS: Child Labor Due Diligence Law	UK: UK Modern Slavery Act 2015	SWITZERLAND: KVI[11] Counter-proposal	USA: Section 1502 US Dodd-Frank Act
01 Degree of legal obligation	Binding (01/2021)	Binding (01/2023)	Binding (03/2017)	Binding (expected for 2022)	Binding (03/2015)	Binding (expected for 2022)	Binding (07/2010)
02 Organizations in scope	EU-based	German[1] >1000[2,3] FTE[4]	French >5,000 FTE[5]	Serving Dutch end users[6]	Business in UK[7] >36M GBP turnover	Certain[8] Swiss-based	US publicly-listed
03 Company obligations	Reporting & limited DD[9]	Reporting & substantial DD	Reporting & substantial DD	Reporting & limited DD	Reporting	Limited reporting & DD	Reporting & limited DD
04 Sanctions	TBD[10] by member states	Fines & non-financial	Fines	Fines & non-financial	Non-financial	Fines	Non-financial

Extensive scope/Degree of regulation Moderate scope/Degree of regulation

INTEGRATING LAW AND MANAGEMENT: A combined legal and strategic perspective

The proliferation of legislative requirements, both on the national and EU level, will force companies to focus more closely on ESG standards, and potential violations of human rights and environmental standards, when managing their supply chains.

However, not all industries are expected to be equally affected by the regulations. BCG analysis suggests that potential supply chain risks for companies will depend on five inherent risk factors (and an effective compliance management system as a mitigating factor):

- Company size and level of international expansion
- Production in emerging and developing countries
- Complexity and level of integration of the global value chain
- Resource intensity of the product mix
- Business relationships in emerging and developing countries

Given these parameters, we anticipate that the companies most likely to be affected by the new regulations are in the commodities, chemicals, and processing industries, as well as agriculture, food, and textile companies. Companies in these sectors tend to conduct large-scale operations in emerging markets, which are on average more likely to be susceptible to human rights and environmental risks, and which may see lower levels of local enforcement than in developed markets. Nevertheless, we do also anticipate that companies will pass their supply chain risk management standards (e. g., by codes of conduct and contract clauses) to their business partner so that also companies in other sectors will gradually be required to address these issues.

1. Including branch offices of foreign companies; 2. Applies from January 2024; 3. >3000 FTE in 2023; 4. Full time equivalent
5. Refers to Group parent and French subsidiaries. However, the law is also applicable to companies with >10,000 FTE worldwide, including subsidiaries
6. Selling or supplying goods or services to Dutch end users; 7. Supplying goods or services
8. No due diligence regarding child labor required if undertaking does not reach at least two of the three following criteria: balance sheet total CHF 20M, revenues CHF 40M, 250 FTE
9. Due diligence; 10.To be defined; 11. Responsible Business Initiative ("Konzernverantwortungsinitiative")

Source: BCG analysis

Given the scope and complexity of the issue, companies cannot handle these legal requirements simply by throwing money at the problem. In contrast, to ensure an effective and cost-conscious management of supply chain risks, they need to follow a consistent risk-based approach, which requires the companies to really understand their value chains. Companies should create and implement an ESG compliance strategy designed to mitigate the relevant compliance risks in their supply chains.

We thus recommend companies to take five steps to manage their supply chain risk:

- Get transparency on potential human rights or environmental risks along your global supply chain
- Evaluate the risk exposure from your operating entities as well as from suppliers/third parties, and build risk cluster
- Develop and implement specific measures for each risk cluster to prevent and mitigate risks, detect misconduct, and continuously improve the supply chain risk management
- Establish tools for continuous monitoring, reporting and documentation, supplemented by on-site audits
- Build and improve governance and organization, including defined roles and responsibilities, to manage supply chain risks on an ongoing basis

ESG compliance needs to be integrated into the company's overall compliance program and communicated to all stakeholders. To devise such a strategy, it will first be necessary to achieve a clear understanding of the company's supply chain network, for example by systematically listing every single one of the company's own sites and its suppliers. A list of supply chain risks should also be drawn up, incorporating potential violations and their respective level of seriousness.

A funnel logic can then be applied, with a small number of sites and third parties exposed to major risks at the top of the funnel. Each entry would detail a particular supply chain risk, together with the internal and external suppliers most closely linked to that risk. All suppliers exposing the company to supply chain risk should be closely examined to ascertain whether they comply with its ESG strategy. For this purpose, the company needs to communicate its ESG compliance rules and standards to its suppliers. At least regarding direct suppliers, companies should integrate its ESG and human rights standards into the supplier contract.

Companies should also negotiate risk management and control mechanisms as well as independent audits, so that they can check whether suppliers follow and adhere to the agreed standards on a regular basis. They should pass compliance standards to their suppliers and should also reserve the right to terminate the business relationship with the respective supplier with immediate effect if these standards are breached. All such steps must be documented. The ESG compliance risk model needs to be adjusted and updated whenever the regulatory framework or business model changes.

This risk management process can be envisaged in five steps (See Exhibit 3).

EXHIBIT 3 | 5 steps you need to take to prepare for the new requirements

STEP 1:
Get transparency on potential human rights or environmental risks along your global supply chain

If a typical manufacturing company just screened its first-tier suppliers, this would involve the unfeasible task of tracking thousands, or even tens of thousands, of companies on an ongoing basis. A rigorous risk-based approach is therefore crucial for ensuring that due diligence is both effective and efficient.

As a starting point, companies need to build an in-depth picture of their business model and supply relationships and establish possible scenarios in which human rights are violated or where environmental norms are disregarded (under the proposed EU Directive, the same will be necessary for issues of good governance, in particular scenarios of bribery). In the case of a manufacturing company with production sites in less developed countries, this could mean, for example, the illegal employment of minors or the pollution of reservoirs from which drinking water is obtained, due to wastewater from the production process.

The aim is first to define the overarching risk categories of possible violations (for example, human rights → child labor violations). These are then further divided into specific sub-risks (for example, human rights → child labor violations → risk of violation of laws protecting minors from exploitation). The sum of the risk categories and sub-risks constitutes the overall map of relevant risks, the so-called risk taxonomy.

Based on this review, the risk indicators for supply chain risks should be set out. These indicators should be specific to the company's business, yet clearly documented and easily comprehensible. Third parties, such as a judge or an auditor, should be able to grasp their meaning. Assessment of risk indicators typically relies on the company's data on suppliers and its own sites, taken for example from its enterprise resource planning (ERP) system. This information is then supplemented by external sources, such as proprietary databases with information on country-specific or industry-specific risk indicators.

Risk indicators might include the location of the supplier or production site, the type of facility (such as production, logistics or administration), and the type of activity performed on the site (unskilled/manual or skilled labor).

When selecting indicators, the rule is to prioritize quality over quantity. To ensure that the subsequent screening process is successful, the data for the selected indicators must either be immediately available, or feasible to calculate. A smaller number of meaningful indicators is therefore the best approach.

STEP 2:
Evaluate the risk exposure from your operating entities and from suppliers/third parties, and build risk cluster

With the benefit of the defined indicators, the actual screening of suppliers and own sites can now begin. The scoring itself should be consistent and, above all, clearly explained. A knowledgeable third party should be able to understand the scoring methodology and reach the same risk score for a given company by applying the methodology themselves. Ideally, therefore, such scoring would be supported by a digital tool. A digital tool typically has several advantages. It is less prone to error and involves a more efficient, user-friendly, and standardized process. In addition, this tool can be used to model risk. For example, it can chart how suppliers are distributed along defined risk clusters and determine whether these correspond to the company's desired distribution and its own risk appetite.

Many financial institutions already use digital solutions for screening potential customers - so-called know-your-customer (KYC) tools. Industry players are using similar tools to monitor suppliers as well. The challenge with such know-your-supplier (KYS) software solutions, however, is that they are usually very comprehensive. They typically incorporate other elements of an end-to-end supplier relationship management process, in addition to the pure risk assessment. Companies that are just starting to screen their suppliers therefore need to be especially aware that the assessment of thousands, or even tens of thousands of legal entities, would take considerable time. To move forward in a results-oriented and risk-based manner, it is thus advisable to include a filter step first.

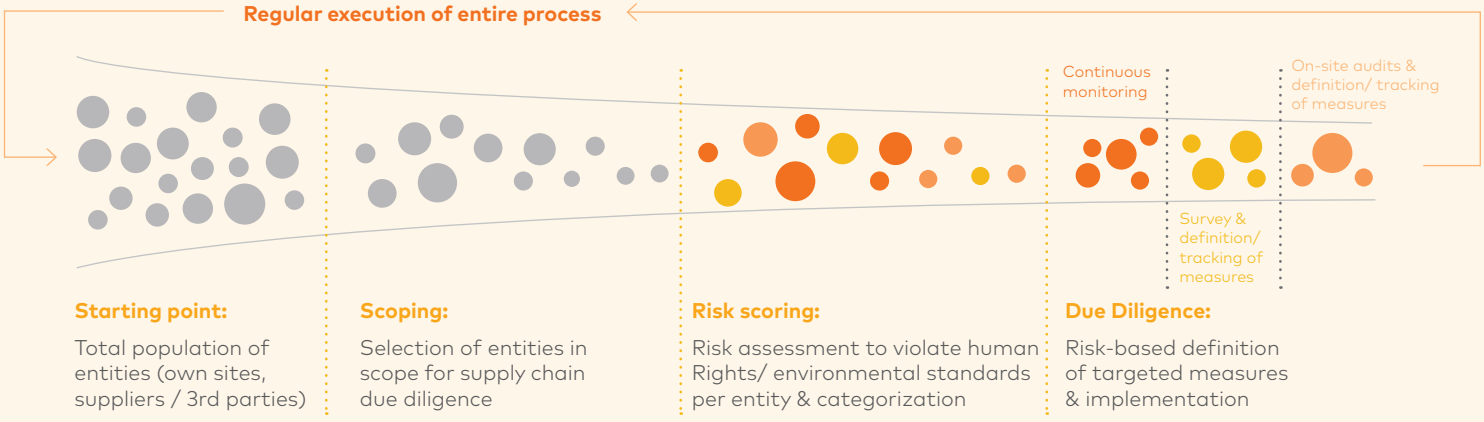
Using a funnel logic, the number of legal entities should first be reduced, for example by excluding a group's non-operative legal entities without employees (shell entities). All entities still in the sample after this weeding out process should then be scored and categorized according to the defined criteria, for example by placing them into high-risk (red), medium-risk (yellow) and low-risk (green) groups. This baseline provides organizations with a quick overview of the number and distribution of high-risk suppliers and operational entities. It also establishes priorities by indicating which suppliers should go through the more sophisticated KYS process first. In this way, the funnel approach allows companies to allocate their resources to those operational entities and third-party suppliers that pose the greatest risk (See Exhibit 4).

The baseline screening, which comes before the actual KYS process, can also be carried out by a separate digital tool. BCG has developed the Sustainability Radar™ specifically for this purpose, enabling companies to generate an overview of their own supply chain risk in just a few weeks, and embark on the next steps with a logical and, most importantly, a risk-based approach. In addition, the risk analysis should always be accompanied by a thorough analysis of legal requirements resulting from applicable supply chain laws in those countries where the company is doing business. The dynamic legal framework for supply chain management needs to be handled in a professional manner.

Finally, it is important that due diligence screenings are not only carried out at the first stage (when new suppliers are onboarded), but that risk ratings and legal requirements are regularly reassessed. Digital tools have a clear advantage for this undertaking. They can take over the regular refresh of the risk assessment in case of non-material changes and trigger human intervention and decision making in case of material changes. Typical material changes that would trigger a review involve negative news. To perform this negative news screening, the tools need (paid) access to the respective databases of news and media sources. If a supplier is flagged, someone finally must decide upon the flagged negative news and to do the final judgement call on it. Also note that a regular risk assessment review not only recognizes the changing risk exposures of individual companies, but also helps to identify more general trends including new regulatory developments.

EXHIBIT 4 | Funnel approach to risk scoring

Best-practice framework for supply chain due diligence



Note: Size of circles illustrate the size of entities based on their generated revenues

STEP 3:

Develop and implement specific measures for each risk cluster to prevent and mitigate risks, detect misconduct, and continuously improve the supply chain risk management

Alongside the scoring mechanism, dedicated packages of measures should be designed for those entities exposed to medium or high risk. These measures would comprise, for example, guidelines and specific supply chain compliance standards, training programs, regular updates in compliance tools and business procedures and processes, or internal controls. They should then be put into practice by the relevant entities, of course considering any already existing measures. In order to secure business risk ownership and to make certain that the process and tool are fit for purpose, it is important to involve the business and the compliance function early on in the conception and implementation of the due diligence. Moreover, companies need to provide clear processes and procedures for due diligence processes for the roles involved.

STEP 4:

Establish tools for continuous monitoring, reporting and documentation, supplemented by on-site audits

Even more critical than defining the packages of measures is verifying their implementation on site. This can be achieved through self-reporting (for example, through a survey to be filled out by company managers), supported by documented evidence, and combined with surprise site audits. The compliance function plays a crucial role in safeguarding these procedures and an effective supply chain management system.

STEP 5:

Build governance & organization, incl. defined roles & responsibilities, to manage supply chain risks on an ongoing basis

Setting up due diligence for a company's value chain is not a one-off enterprise but a permanent endeavor. Procedures and processes should therefore be embedded within the company at the board level as part of the general compliance risk strategy and by means of appropriate organization and governance. In line with current legal requirements and with stakeholders´ expectations, the management board needs to provide for a clear definition of roles, responsibilities, reporting lines, defined frequency of reporting, and escalation channels.

CONCLUSION

National and international laws on company supply chains have proliferated in recent years, a trend that is likely to continue in line with increasing scrutiny by stakeholders and the public. These laws expound numerous obligations for companies with respect to safeguarding human rights, protecting the environment and issues of good governance (particularly the prevention of bribery). Business leaders cannot afford to downplay the potential impact of non-compliance, involving substantial fines and devastating reputational damage. By taking five logical steps to prepare for their new obligations, companies can expect to mitigate their supply chain risks in an efficient and cost-effective way over a sustained period of time. Both a rigorous risk-oriented approach that focuses on the most significant risks and legal requirements, and the use of appropriate digital tools and compliance standards for continuous risk assessment, are key success factors.

Contacts

Boston Consulting Group GmbH

Dr. Katharina Hefter
Managing Director & Partner
BCG Berlin
hefter.katharina@bcg.com

Dr. Bernhard Gehra
Managing Director & Senior Partner
BCG Munich
gehra.bernhard@bcg.com

Dr. Julia Lingel
Partner
BCG Munich
lingel.julia@bcg.com

Florian Meier
Project Leader
BCG Berlin
meier.florian@bcg.com

CMS Hasche Sigle

Dr. Joachim Kaetzler
Partner, Attorney at Law
CMS Frankfurt am Main
joachim.kaetzler@cms-hs.com

Prof. Dr. Martin Schulz
Of Counsel, Attorney at Law
CMS Frankfurt am Main

Professor at the German Graduate School of Management and Law
martin.schulz@cms-hs.com

Dr. Christoph Schröder
Counsel, Attorney at Law
CMS Hamburg
christoph.schroeder@cms-hs.com

Peter Rempp
Senior Associate, Attorney at Law
CMS Cologne
peter.rempp@cms-hs.com

BCG BOSTON CONSULTING GROUP

CMS law·tax·future