MANAGING SUPPLY CHAIN RISK

An update on legal and strategic requirements in light of recent EU developments

September 2022

BCG BOSTON CONSULTING GROUP

CMS law·tax·future

In June 2021, BCG and CMS published a White Paper entitled "Managing Supply Chain Risk – A legal and strategic perspective". In view of the rising number of laws obligating companies to prevent and mitigate risks relating to human rights and the environment in their supply chains, the White Paper provided an overview of selected laws, and offered practical guidance on how to manage such risks.

One notable example of national supply chain regulation is the German Supply Chain Due Diligence Act ("German Supply Chain Act"), which was adopted in June 2021 and will come into force on 1 January 2023. The German Supply Chain Act sets out new due diligence obligations for in-scope companies and their management, such as conducting a risk analysis, issuing a policy statement, implementing preventive measures and remedial actions, continuously documenting the fulfillment of due diligence obligations, and the publication of a yearly report.

In addition to national supply chain regulation, the protection of human rights and the environment is also the subject of various legislative initiatives at the European Union ("EU") level. In February 2022, the European Commission published its proposal for a directive on corporate sustainability due diligence ("EU Proposal"), which sets out due diligence obligations that go beyond the German Supply Chain Act.

Many companies are already preparing for the implementation of these new requirements. Our new paper therefore has two objectives. First, we will compare the EU Proposal with the German Supply Chain Act in order to shed light on the expected additional requirements. We will then provide an overview of the main challenges for companies in implementing the relevant requirements, together with some of the practical lessons we have learned about this implementation from the standpoint of both legal and strategic consulting practices. These challenges include:

01. Developing a company-specific risk concept and analysis, first identifying pertinent human rights and environmental issues, and then acting on these issues by defining key risk indicators ("KRI") and formulating a scoring model;

02. Implementing measures and monitoring tools, focusing on salient human rights and environmental risks and using an appropriate range of clear, practicable and effective measures, rather than trying to eliminate every risk;

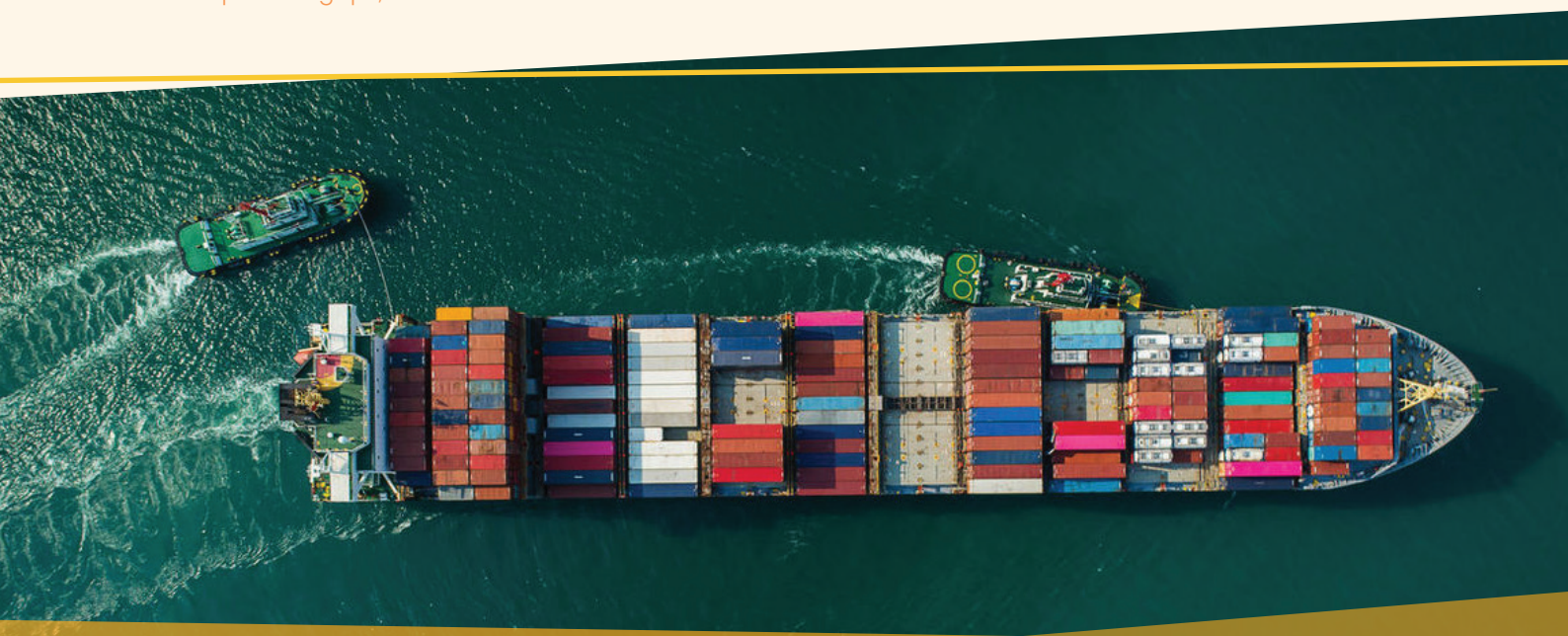
03. Preparing a company-specific policy statement, which requires central coordination and orchestration of the necessary process steps in order to prevent gaps;

04. Securing alignment with overall company purpose and strategy, integrating relevant human rights risk and environment compliance issues into a broader strategy and framework with regard to sustainability and environmental, social and governance ("ESG") criteria;

05. Creating an adequate complaints procedure, which aims to complement existing whistleblowing systems and open up (new) input channels for relevant third parties;

06. Allowing ample scope for scalability of the approach in the light of a possible further tightening of regulation due to the recently published EU Proposal;

07. Building efficient project management, with an emphasis on coordinating and aligning activities across the relevant departments (such as in Procurement or Human Resources ("HR")), and on a close and cross-functional cooperation of the departments involved, such as Procurement, HR, Compliance, IT, and Sustainability as requirements of the law can only be conquered jointly.



MANDATORY HUMAN RIGHTS AND ENVIRONMENTAL DUE DILIGENCE:

Comparing the German Supply Chain Due Diligence Act and the EU Commission's Proposal for a Corporate Sustainability Due Diligence Directive

The below table shows that the EU Proposal goes beyond the German Supply Chain Act in the following ways:

- The EU Proposal also applies to smaller companies
- It also applies to many non-EU companies (extraterritorial effect)
- It addresses the climate and covers more treaties on human rights and the environment
- It requires all in-scope companies to exercise due diligence vis-à-vis their subsidiaries
- It fully covers the downstream value chain
- It provides for civil liability
- It emphasizes the responsibility of directors

	GERMANY	EU
Name	Act on Corporate Due Diligence Obligations for the Prevention of Human Rights Violations in Supply Chains *(Lieferkettensorgfaltspflichtengesetz – LkSG)*	Proposal for a Directive of the European Parliament and of the Council on Corporate Sustainability Due Diligence and amending Directive (EU) 2019/1937
Next steps	• To be applied by larger companies from 1 January 2023 • To be applied by smaller companies from 1 January 2024 • Likely to be amended due to EU directive during its transposition period	• Awaiting voting of European Parliament and of Council • Upon entry into force, two-year transposition period begins • To be applied by larger companies upon expiry of transposition period • To be applied by smaller companies in high-impact sectors upon expiry of further two-year period
Personal scope	Enterprises which have • their central administration, principal place of business, administrative headquarters, statutory seat, or branch office in Germany *and* • at least 3,000 employees in Germany (from 2024: at least 1,000)	Companies which 01 are formed in accordance with the legislation of a Member State and have a. more than 500 employees and a turnover of more than €150 million or b. more than 250 employees and a turnover of more than €40 million, provided that at least 50% of this turnover was generated in one or more high-impact sectors 02 are formed in accordance with the legislation of a third country and generate a. a turnover of more than €150 million in the EU or b. a turnover of more than €40 million in the EU, provided that at least 50% of its worldwide turnover was generated in one or more high-impact sectors
Legal form	Not relevant	• Corporations • Partnerships held exclusively by corporations • Financial undertakings

	GERMANY	EU
When it comes to determining the number of employees, do only employees of the respective enterprise or company count?	In principle yes, but employees of affiliated companies are attributed to the ultimate parent company *(Obergesellschaft)*	Yes
Are subsidiaries the object of due diligence?	Only for the ultimate parent company, and only in the event of decisive influence on the subsidiary	Yes, in the case of a controlled undertaking
Are companies less responsible for the actions of indirect suppliers?	Yes, due diligence obligations are in principle only triggered upon substantiated knowledge	Yes, regarding civil liability
Is due diligence also to be applied downstream?	No (with certain exceptions)	Yes
Objects of protection	• human rights (11 conventions) • environment (3 conventions)	• human rights (22 conventions) • environment (7 conventions) • climate – however, not as an object of due diligence, but as an aspect to be considered when larger companies plan their business model and strategy
Due diligence obligations	• Establishing a risk management system • Designating person(s) responsible for monitoring risk management • Performing regular risk analyses • Issuing a policy statement • Laying down preventive measures • Taking remedial action • Establishing a complaints procedure • Documentation • Reporting	• Integrating due diligence into corporate policies • Identifying actual or potential adverse impacts • Preventing and mitigating potential adverse impacts, and bringing actual adverse impacts to an end and minimizing their extent • Establishing and maintaining a complaints procedure • Monitoring the effectiveness of due diligence policy and measures • Publicly communicating on due diligence
Provisions on obligations/ remuneration of directors	• Senior management must seek information about the work of the person(s) responsible for monitoring risk management. • Senior management must adopt the policy statement on human rights strategy.	• Directors must take into account sustainability matters when fulfilling their duty to act in the best interest of the company. • Directors are responsible for putting in place and overseeing all due diligence actions, in particular due diligence policy. • Directors must adapt corporate strategy to take into account actual and potential adverse impacts and certain measures. • Under certain circumstances, adopting a plan to make the business model and the strategy of the company sustainable must be taken into account when setting criteria for the variable remuneration of a director.

	GERMANY	EU
Supervisory authority	Federal Office for Economic Affairs and Export Control *(Bundesamt für Wirtschaft und Ausfuhrkontrolle – BAFA)*	To be designated by each Member State
Sanctions	Administrative fine of • up to €100,000 / €5 million / €8 million (depending on the type of infringement) • up to 2% of the average annual worldwide turnover of all natural and legal persons operating as a single economic entity – only for certain infringements and if such turnover exceeds €400 million As a rule, the award of public contracts also to be excluded • for up to three years • only in the case of a final and binding fine of a certain minimum amount (depending on the type of infringement)	• To be determined by each Member State • Sanctions must be effective, proportionate, and dissuasive. • When pecuniary sanctions are imposed, they shall be based on the company's turnover. • Any decision of the supervisory authority containing sanctions must be published (naming and shaming). • Companies applying for public support must certify that no sanctions have been imposed on them.
Civil liability	• Liability for violation of due diligence obligations explicitly excluded • Liability under German general tort law questionable • Liability under foreign law possible • No provisions on applicable law. In principle, the law of the country in which the damage occurs is applicable • Special capacity to sue for trade unions and non-governmental organizations ("NGOs")	• Liability for violation of certain due diligence obligations explicitly prescribed • No provisions on burden of proof • Liability regime under directive applies even if law of non-Member State is applicable

TYPICAL CHALLENGES AND THE LESSONS LEARNED ON THE JOURNEY SO FAR

Our practical experience working with multiple clients across different industries tells us that companies tend to face similar challenges, in both the legal and strategic spheres, when managing supply chain compliance. The principal challenges are detailed below, together with the lessons on best practice that we have picked up along the way.

01 | Company-specific risk concept and analysis

A period of legal uncertainty for companies often ensues as they contemplate the implementation of these new regulatory requirements. Instead of seeking one ideal solution (the silver bullet) to meet these requirements, we would recommend a thorough process that starts with a top-down risk analysis of all the relevant risks that the company faces.

With the German Supply Chain Act, the first stage is to identify pertinent human rights and environmental risks in the operations of the company[1] and its direct suppliers[2]. Once they have been identified, companies need to operationalize the management of these human rights and environmental KRIs. These KRIs facilitate measurement, ultimately enabling a risk scoring model to be established.

The German legislator has made it clear that any concrete human rights risks (and the environmental risks that are also covered) are always particular to the company. Each company therefore has to identify and manage the risks in its own supply chain and its own value creation processes, and to understand where the rights of its own employees, suppliers and other third parties, such as residents, may be threatened.

Practical experience suggests that it is advisable to carry out the top-down analysis right at the start of the process. Although this will involve significantly more effort than simply setting out a generic list of risks, it will help to prevent unnecessary time and money being wasted at a later juncture on managing risks that pose little threat to the organization. An approach that prioritizes risks is both possible and recommended[3]. If they just make use of a generic list of potential human rights violations on the other hand, companies may expend superfluous effort in their endeavor to comply with the law, while not focusing sufficiently on the precise risks they need to address.

Another important undertaking is to determine the appropriate scope of suppliers. One way to prioritize risks is to appraise the importance of a supplier to the company. A typical measure of this importance is the amount of money spent on its products or services relative to other suppliers. Therefore, if a company has identified a group of suppliers posing an equivalent level of risk, and if time and/or resources are limited, then it would be pragmatic to start by dealing with the suppliers that involve the highest expenditure. However, it is crucial that such prioritization is rule-based and documented in a way that is comprehensible for third parties, such as supervisory authorities.

When setting up the risk model, care must be taken to ensure that the data sources are known and available for each risk. Typical examples of such data include information about the company's own suppliers of potentially critical raw materials such as rare earths, or country-specific human rights indices sourced through third-party vendors for the locations where the company operates. The more risks that are covered, the higher the effort involved in collecting the data - another reason to focus only on the most relevant risks. Companies must also ensure that they understand how long it takes to produce the data so that they can meet statutory reporting deadlines.

1. Crucially, however, the proposed EU Directive casts its net more widely. Under this directive, an in-scope company is obliged to carry out due diligence obligations (such as risk analysis) not only with respect to its own operations and the operations of its subsidiaries, but also to such companies with which it has an established business relationship (the latter being rather broadly defined). The risk analysis of relevant human rights and environmental issues ought therefore to be applied to the entire supply chain.

2. The risk analysis must also be extended to indirect suppliers in the event that the company becomes aware of facts which indicate the violation of human rights or certain environmental obligations.

3. As stated in the combined FAQ of the Federal Ministry for Economic Affairs and Climate Action, the Federal Ministry of Labour and Social Affairs, and the BAFA , companies may adopt a tailored approach which addresses specific human rights risks in their own operations and supply chains.

02 | Measures and monitoring tools

Based on their individualized risk analysis, companies need to develop specific measures and monitoring tools to oversee and mitigate the human rights risks that are relevant to them. Our overall experience of risk and compliance management suggests that an achievable number of clear, practicable, and effective measures promises a significantly higher level of protection than drowning every conceivable sub-risk in a multitude of measures. The management of human rights risk is no exception to that rule.

That being the case, companies would benefit from classifying their suppliers, as well as their own legal entities, subsidiaries, or production sites, into different risk clusters based on a scoring model. These clusters could be labeled as low, medium, or high risk.

For the first part of this process, such a scoring model could use publicly observable (though not necessarily free of charge) data, such as company expenditure and revenue, and data points from paid databases such as Verisk Maplecroft which provide human rights risk data for specific regions and/or industries. For those entities which are classified as medium to high risk, additional questionnaires should be sent to the entities in order to glean a clearer understanding of their current control environment.

While companies cannot simply omit suppliers (or indeed their own legal entities, subsidiaries, or production sites) from the overall analysis, such a clustering can facilitate a more efficient use of resources when it comes to the later stage of developing risk mitigating measures. It allows companies to focus on those suppliers, entities and sites that pose the greatest threat.

The risk clustering can also be used to put in place specific sets of measures for each group. For example, any supplier, regardless of their risk scoring, should be asked to confirm a supplier code of conduct, while the high-risk cluster may, among other measures, be subject to an additional audit plan that includes regular site visits.

03/04 | Company-specific policy statement and alignment with company purpose and strategy

Under the German Supply Chain Act, senior management is required to issue a policy statement (Grundsatzerklärung) on its strategy regarding human rights and environmental issues. Based on its own risk analysis, the company´s expectations regarding human rights and environmental issues towards should be communicated to employees and suppliers.

In comparison, the EU Proposal sets out the responsibility of management for human rights and environmental issues in a more detailed way. Directors must consider the short-term, medium-term, and long-term consequences of their decisions on sustainability issues, including the consequences for human rights, climate change and the environment. National law would be responsible for dealing with any breaches of these duties. Moreover, in certain circumstances, the company must take climate change into account when setting its variable remuneration for directors.

When it comes to the policy statement required under the German Supply Chain Act, some companies tend to want to copy and paste a generally applicable solution. However, a note of caution should be sounded here. When compiling the information for the policy statement, companies should find a balance between achieving the transparency required by the legislator and the supervisory authority, and the risk of making exaggerated promises and therefore setting the bar too high.

A further point worth making is that the policy statement on human rights should be viewed in the context of a company's overall ESG strategy. Capital markets and rating agencies may raise their eyebrows if a company were to proclaim an ambitious ESG strategy to improve its own ESG rating, but later issue a much less ambitious policy statement. The level of aspiration set should be consistent with previous communication.

Moreover, the policy statement must accurately reflect the main features of the human rights-based risk management system in a way that is comprehensible to third parties, such as representatives of the BAFA, without making unrealizable promises.

Another major challenge is that multiple companies within the same corporate group may need to apply the German Supply Chain Act and hence must each issue their own policy statement. Central oversight and coordination are necessary to ensure that all policy statements have the same, group-wide look and feel, while each policy statement must also manage to reflect the individual risk exposure of the subsidiary. This entails a group-wide preparation process, timeline and sign-off by respective executives.

05 | Complaints procedures

One significant challenge is the implementation of an appropriate complaints procedure that enables individuals to report human rights and environment-related risks or violations resulting from the business activities of the company or of a direct or indirect supplier.

The German Supply Chain Act lays out several legal requirements detailing exactly how such a complaints procedure should be set up. Any failure to meet these requirements can result in an administrative offence with a fine of up to €8 million. A company can either entrust internal personnel with implementing these requirements, or participate in an appropriate external complaints procedure.

The German Supply Chain Act also demands that the rules of the complaints procedure should be publicly available in text form. That is to say there must be clear and comprehensible information on accessibility and responsibility. The persons entrusted with managing the procedure must offer a guarantee of impartiality, and are bound to secrecy. The German Supply Chain Act sets out certain other general requirements: the procedure should be accessible to potential parties involved; it must maintain confidentiality of identity; and it must ensure effective protection against any disadvantage or punishment due to making a complaint. The procedure must be reviewed at least once a year, or sooner still if the company experiences or anticipates significantly altered risk circumstances in its own business area or at a direct supplier.

Particular attention in the German Supply Chain Act is placed on the importance of ease of access to the complaints procedure. Indirect suppliers must not be ignored here, as this stipulation also applies to complaints about their activities.

Companies should view these new requirements in conjunction with the new legal framework for whistleblowers under the EU Whistleblowing Directive, and the corresponding national implementation laws. In the Federal Republic of Germany, the government presented a corresponding draft in mid-April.

With the benefit of practical experience, we can confirm that following the relevant requirements of the German Supply Chain Act in conjunction with those of the EU whistleblowing framework is expedient and efficient, given their similarities. The integrated complaints procedure and whistleblower system must be comprehensive and easily accessible, for example via mail, phone, website access or contact with a designated individual.

Given the different thresholds for the application of the two new laws, the implementation of the complaints and whistleblowing system must be carefully planned. As with all information received by a whistleblowing system, information on possible human rights violations or environmental violations covered by the law needs to be handled by competent personnel, checked for its validity, and followed up appropriately if such action is warranted.

If an investigation does indeed reveal human rights violations, these must of course be remedied immediately, and reparations have to be made to the injured parties. As with the rest of the whistleblower system, lessons should be learned and conclusions drawn with regard to any systemic weaknesses. Shortcomings can then be rectified through appropriate adjustments to processes, or the introduction of new controls.

06 | Scalability of the approach

As we have seen, the German Supply Chain Act is part of a regulatory trend, which is set to be extended throughout Europe with the EU Proposal. Maintaining a sufficiently flexible approach when implementing the German requirements is therefore critical, as it allows more far-reaching requirements, such as those from the EU, to be integrated at a later date.

This principle can be illustrated by means of a practical example. The scope of companies covered by the German law incorporates companies with more than 3000 employees from 2023, and 1000 employees from 2024. In any group of companies, a system should be introduced whereby the precise number of employees in each of the companies is checked at set regular intervals. This will determine which group companies at that point exceed the threshold number and are therefore themselves covered by the law, and which fall below the criteria and are outside the scope of the law.

To ensure that this process can be easily repeated, the information required needs to be well defined, the internal company sources for the information should be known, and the necessary time to obtain the information should be reasonable. In this way, companies only need to adjust the country scope and/or threshold values to identify newly affected group companies when new laws and regulations, such as the EU Proposal, enter into force.

07 | Efficient project management

The successful implementation of the supply chain compliance management system is only possible if all relevant departments work hand in hand. These include, for example, the Compliance department, Procurement, Human Resources, and IT.

To make the approach efficient and effective, harmonization with the general approach to risk and compliance management is crucial. The risk categories for human rights risk should utilize the same methodology as in all other areas of the company's risk management.

Moreover, answers to the following questions should be similar whether they concern human rights risk or any other. What defines a material risk? How are likelihood and impact assessed – for example, will a three-level or a five-level scheme be used, or something different? How often are risks updated for internal reporting and which templates are used?

Should this consistency be absent, the information produced by subsidiaries, for example, may not be comparable because they are not based on similar standards. Putting together a single report for senior management and the authorities would also be difficult to accomplish.

As with the policy statement, such consistency relies on coordination from the center. Indeed, a central management body can secure uniformity and the desired level of quality, while also acting as a single conduit between the various stakeholders in the project and senior management. In this way, decision making and the general approach throughout the company can be properly aligned.

CONCLUSION: Navigating the pitfalls

Although both the German Supply Chain Act and the EU Proposal have both seen the light of day only recently, many companies are already reacting to their contents. We have seen that different companies encounter similar legal and organizational pitfalls as they set about this work. Companies seeking to hone the effectiveness of their response, or newly embarking on this journey, can learn invaluable lessons from the experience that others in their position have already gained.

By carefully considering all the day-to-day complexities of supply chain risk management, and navigating the relevant and already known pitfalls, they can implement smooth and effective processes that will ensure compliance.

The new requirements, which open up the potential for severe sanctions if not properly implemented, are a challenge for any responsible entrepreneur or company executive. But with a pragmatic approach focused on the most relevant risks for the company, by implementing a manageable number of effective measures, and through clear governance and oversight, it is possible to deal with the law successfully. However, for the risk scoping and scoring logic to be accepted by the authorities, they must be sufficiently documented and logically justified according to the company's business model and geographical footprint.

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

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

Dr. Julia Gebhardt
Managing Director & Partner
BCG Munich
gebhardt.julia@bcg.com

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

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

Prof. Dr. Martin R. Schulz
Counsel, Attorney at Law
CMS Frankfurt am Main
martin.schulz@cms-hs.com
Professor at the IU International
University of Applied Sciences

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

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

ABOUT BCG

Boston Consulting Group partners with leaders in business and society to tackle their most important challenges and capture their greatest opportunities. BCG was the pioneer in business strategy when it was founded in 1963. Today, we help clients with total transformation—inspiring complex change, enabling organizations to grow, building competitive advantage, and driving bottom-line impact.

To succeed, organizations must blend digital and human capabilities. Our diverse, global teams bring deep industry and functional expertise and a range of perspectives to spark change. BCG delivers solutions through leading-edge management consulting along with technology and design, corporate and digital ventures—and business purpose. We work in a uniquely collaborative model across the firm and throughout all levels of the client organization, generating results that allow our clients to thrive.

ABOUT CMS

The challenges of today and tomorrow require courageous, independently-thinking and future-facing personalities who are as diverse in the community as the problems of our clients. As the world reinvents itself, becomes more complex and requires faster reactions, we stand up for your interests and pursue them with you.

CMS is one of the largest commercial law firms in the world. More than 5,000 lawyers work together in cross-border teams. In more than 70 cities and more than 40 countries where we are present, we represent our clients' interests with the same dedication and commitment to quality. This means that CMS is optimally positioned to provide you with the precise legal and tax-related know-how and regional market knowledge that you need to stay competitive and achieve your business goals – wherever your business is.

BOSTON CONSULTING GROUP

CMS law·tax·future