Contents

Preface ................................................................................................................. 7
About the authors .............................................................................................. 8

1. Corporate compliance .................................................................................. 10
   1.1 What is compliance? ............................................................................ 11
   1.2 Why is compliance important? ............................................................. 13

2. Integrating compliance into a company ..................................................... 16
   2.1 Risk Assessment .................................................................................. 17
   2.2 Appoint responsibility for legal compliance ......................................... 19
       2.2.1 Primary responsibility ................................................................. 19
       2.2.2 Delegation to a committee ......................................................... 20
       2.2.3 Responsibility for day-to-day operations ................................... 21
   2.3 Establish standards and procedures ..................................................... 24
   2.4 Implement ............................................................................................. 26
       2.4.1 Communicate ............................................................................... 26
       2.4.2 Training ....................................................................................... 27
   2.5 Periodic review ..................................................................................... 29
       2.5.1 Monitoring and auditing .............................................................. 30
       2.5.2 Reporting .................................................................................. 31
   2.6 Handling concerns/Whistleblower system ............................................ 31
       2.6.1 Whistleblower system ................................................................ 31
       2.6.2 Investigation ............................................................................... 32
       2.6.3 The Mediation and Complaints-Handling Institution for
             Responsible Business Conduct.................................................... 33
   2.7 External Reporting ............................................................................... 33
       2.7.1 Financial Reporting .................................................................... 35
       2.7.2 Non-Financial Reporting .............................................................. 36

3. What happens in the case of non-compliance? .......................................... 38
   3.1 Receiving the allegation and determining a course of action ................. 39
   3.2 Internal investigation ......................................................................... 39
   3.3 Self-reporting and other follow-on measures ...................................... 41
       3.3.1 Self-report .................................................................................. 42
       3.3.2 Disciplinary measures ................................................................. 43
       3.3.3 Modifying the compliance programme ....................................... 43

4. Areas relevant to compliance ..................................................................... 44
   4.1 Competition Law .................................................................................. 45
       4.1.1 Competition Law: Overview ....................................................... 45
       4.1.2 Anti-competitive Agreements ...................................................... 45
       4.1.3 Abuse of Dominant Position ....................................................... 46
Preface

What is compliance? Why is compliance important to a company? How can a compliance programme be developed and integrated into a company?

These questions, in addition to others, are answered in this practical guide on corporate compliance, which is aimed to assist people working with compliance in a Danish company.

In today’s increasingly globalised world, where companies operate in a complex regulatory environment, developing and integrating an effective compliance programme is a necessity. The issue of compliance affects large multinational companies and small and medium sized companies alike. Several jurisdictions are enlarging the scope of their laws so that a Danish company may, for example, be liable for the actions of its agent paying facilitation payments in Azerbaijan. Furthermore, public authorities are increasing their enforcement efforts, both in the form of conducting investigations and heightening the level of fines and/or imprisonment penalties.

This practical guide introduces the reader to compliance and then in a step-by-step manner explains how compliance can be integrated into a company, covering the topics including conducting a risk assessment, appointing responsibility for compliance, establishing standards and procedures, implementation, periodic review, handling concerns and establishing a whistleblower system and external reporting. Examples and suggestions are provided along the way to illustrate how these issues are handled in practice.

What to do in the case of non-compliance, despite a compliance programme having been in place, is also addressed in the practical guide. Issues such as how a company receives complaints, whether to conduct an internal investigation and considering the option of self-reporting are all relevant to a company when handling instances of non-compliance.

This practical guide concludes with a brief overview of compliance concerns in several areas – competition law, anti-corruption, export control, data privacy, labour standards and human rights, and tax – which are typically the areas where companies face compliance risks.

With the challenging compliance regulatory environment companies currently face, this practical guide will likely generate interest in the boardrooms and promote a culture of compliance within the company.
About the authors

**Camilla C. Collet** (Gorrissen Federspiel, partner, head of Corporate/M&A) has extensive experience advising Danish and international businesses on contractual matters, mergers and acquisitions and compliance issues, specialising in anti-corruption, in conjunction with lecturing on these areas. Further, Camilla has extensive transactional experience within life sciences, insurance and other regulated industry sectors.

**Martin André Dittmer** (Gorrissen Federspiel, partner, head of EU & Competition) has extensive practical experience within Community law, including advising and training businesses on competition law compliance, in addition to lecturing on EU and Danish competition law. Further, Martin holds special insight into the energy, airline, shipping and telecommunications sectors.

**Emily Laura Crawford** (Gorrissen Federspiel, legal advisor, Compliance & CSR) has experience with compliance, human rights and business and CSR. A trained lawyer from Australia, Emily's interest lies with advising businesses on sustainable solutions.

Contact information

**Camilla C. Collet**
Partner
T +45 33 41 42 09
M +45 24 28 68 09
ccc@gorrissenfederspiel.com

**Martin André Dittmer**
Partner
T +45 33 41 41 43
M +45 24 28 68 27
mad@gorrissenfederspiel.com
This paper is a practical guide on compliance, targeted at people working with compliance in a Danish company, for example the compliance officer or chief financial officer. Although compliance is an international topic and often covers jurisdictions outside of Denmark, this guide is written from a Danish perspective. The guide is a guide on compliance in general and does not address the specific compliance rules which apply to individual sectors, such as financial institutions.

Following an introduction to compliance in chapter one, chapter two outlines how compliance can be integrated into a company in a step-by-step manner. Integrating compliance includes conducting a risk assessment, appointing responsibility for compliance, establishing standards and procedures, implementation, periodic review, handling concerns and establishing whistleblower systems, and external reporting. The guide looks at each step from a practical perspective and provides a number of examples and/or suggestions in order to illustrate how companies can implement each stage.

Chapter three looks at what companies can do in the case of non-compliance, despite having a compliance programme in place. Issues such as receiving complaints, whether to conduct an internal investigation and considering the option of self-reporting are discussed.

Lastly, several compliance areas that are often relevant for companies — competition law, anti-corruption, export control, data privacy, labour standards and human rights, and tax — are briefly described. The specific issues that companies should consider when drafting a compliance programme for each area are also highlighted.

1.1 What is compliance?

Compliance refers to a company complying with all applicable laws, regulations, standards, contractual obligations and requirements imposed by public authorities. It can also include compliance with internal ethical standards. To ensure that a company complies with such relevant laws and regulations, it should establish a compliance programme, which should preferably consist of a policy, code(s) of conduct and supporting procedures. The compliance policy presents the company’s overarching policy on compliance whereas the code(s) of conduct is normally a more detailed manual designed to assist in implementing the policy. Supporting procedures include implementation tools such as training, monitoring and auditing the compliance programme, reporting mechanisms, and complaints handling procedures.
Compliance does, however, go deeper than merely establishing a compliance programme. Today, companies are expected to demonstrate that there is a *culture* of compliance, or integrity, within the company itself. The US Sentencing Guidelines Chapter 8, which concerns the sentencing of organisations, reflects this expectation with its explicit reference to ethics as part of a compliance programme. It is now expected that corporate leaders foster a culture of compliance within the company. Essentially, it is not sufficient for the leadership of a company to merely establish a compliance programme: it must also promote and support a strong ethical culture. A culture of compliance will ensure that the compliance programme is in fact effective.

### 1.2 Why is compliance important?
Compliance is important on a number of levels for the company. First and foremost, companies are under a legal obligation to comply with the law. This legal obligation suggests that companies should take compliance seriously and develop mechanisms to ensure that it does in fact comply with the law.

In addition to a company’s legal obligation to comply with the law, there are further, persuasive reasons for a company to prioritise compliance, namely concerning the significant consequences that follow in the case of non-compliance:

**Penalties**

If a company is found liable for non-compliance, the public authorities can impose significant penalties on the company itself and in some cases on the persons found responsible. For example, the fines that can be imposed on the company in the event of a breach of EU competition law can be up to 10% of the company’s worldwide annual turnover. For this reason alone, many companies place high importance on developing compliance systems concerning competition law. Another example is the recent case of BNP Paribas, where the French bank was fined a record USD 9 billion by the US authorities for breaching sanctions against US-blacklisted Sudan, Iran, Burma and Cuba between 2002 and 2012. Key units of BNP Paribas are also suspended for one year to process U.S. dollar payments.¹

Personal liability, in conjunction with corporate liability, is also a real possibility, especially when public authorities investigate cases of corruption. Personal liability can be a fine or even imprisonment. In a recent case, GlaxoSmithKline’s former head of its China operations was given a three year suspended sentence for convictions of bribery.\(^2\)

**Civil damages**

In addition to penalties imposed by public authorities, the company can face civil actions for damages. Individual or class actions against the company or the individuals responsible are a real risk. Recent developments highlight this possibility; the EU Parliament in November 2014 passed a directive that will make it easier for those harmed by infringements of EU antitrust law to bring an action for damages.\(^3\) Furthermore, in the U.S. board members may be held liable for breach of their fiduciary duties regarding the Foreign Corrupt Practices Act, by not establishing or monitoring appropriate anti-corruption compliance programmes or not thoroughly investigating allegations of FCPA violations.\(^4\) In the European context, the Council of Europe Civil Law Convention on Corruption requires states to provide legal remedies, including the right to obtain full compensation for damages, for persons who have suffered damage as a result of acts of corruption.\(^5\) Civil damages can be significant and the legal costs involved in defending such an action can also be considerable.

**Reputation**

Possibly the most significant consequence resulting from a breach in compliance is the potential damage caused to the company’s reputation. A company’s reputation is often an important corporate asset, and increasingly seen as a major source of competitive advantage, yet it is extremely difficult to protect. Furthermore, compliance can play an especially important role in supporting a company’s reputation. A survey of 269 senior risk managers found that 29% of companies cite failures to meet regulatory or legal obligations as a major source of reputational risk, with the majority citing compliance as the biggest threat to reputation.\(^6\)

Reputational problems can be the most costly to a company in financial terms, and the most difficult to repair. In the vitamin cartel case, Hoffman-La Roche, the world’s largest vitamin producer, was found guilty by the EU Commission of being the primary instigator and beneficiary of a cartel with seven other vitamin companies, and fined along with the other cartel members. In addition to paying a fine of EUR 462 million, Hoffman-La Roche also paid fines in the U.S., Canada and Australia. However, despite the weighty fines and consequent civil actions from customers, the most damaging consequence was arguably the serious bad-will caused to the company’s brand. In 1999 it was ranked first place on ‘The Top 100 Corporate Criminals of the 1990s’ by the American magazine Multinational Monitor; a reputation difficult to overcome. The consequences outlined above highlight the significant costs to a company that can flow from non-compliance. The importance of compliance cannot be stressed enough in today’s environment. The risks of non-compliance are present and have increased in recent years: multinational companies employing thousands of employees, engaging with multiple business partners and conducting extensive operations throughout the world are particularly vulnerable to non-compliance risks. Maintaining a strong compliance programme can be a challenge, and yet enforcement by public authorities is actually increasing. However, the good news is that public authorities look favourably upon companies that have implemented compliance programmes, and may reduce the penalties imposed where an instance of non-compliance is discovered. Implementing compliance into a company therefore makes good business sense on a number of grounds.


\(^4\) For an explanation of directors’ duty of care including oversight responsibility for legal compliance, see for example Caremark Int’l. Inc., 698 A.2d 269 (Del. Ch. 1996) where the Delaware Court of Chancery ruled that a director’s duty of care includes an obligation to ensure adequate corporate oversight systems are in place, and directors may be held liable for losses caused by legal non-compliance if the company has not implemented control mechanisms to prevent such losses.

\(^5\) The Council of Europe Civil Law Convention on Corruption (1999) article 3. Note: Denmark signed the Convention on 4 November 1999 but has not ratified it – the Convention has therefore not entered into force in Denmark.

2. Integrating compliance into a company

2.1 Risk Assessment

Before creating compliance procedures, a company must first undertake a comprehensive risk assessment. The risk assessment will enable the company to firstly identify what existing and emerging risks it faces, both internally and externally, and secondly assess and prioritise these risks. Accordingly, the compliance programme should be tailored to reflect the risk profile of the company.

The initial stage – identifying the risks – should take into account a number of factors in order to capture a broad overview of all the compliance risks that the specific company faces.

To take a risk assessment in the area of corruption as an example, the UK Government has listed commonly encountered external risks a company should consider. These risks include:

- **Country risk**: perceived high levels of corruption (see Transparency International’s Corruption Perception Index); absence of anti-bribery legislation and implementation; failure from the foreign government, media, local business community and civil society to effectively promote transparent procurement and investment policies.

- **Sectoral risk**: some sectors, such as the extractive industries, public contracts and construction, pharmaceutical and healthcare, are higher risk than others.

- **Transaction risk**: certain transactions give rise to higher risks, for example charitable or political contributions, licences and permits, and transactions relating to public procurement.

- **Business opportunity risk**: risks might arise for example in high value projects or with projects involving many contractors or intermediaries, or with projects which are not apparently undertaken at market prices or which do not have a clear legitimate objective.

- **Business partnership risk**: certain relationships may involve high risk, for example the use of intermediaries in transactions with foreign public officials, consortia or joint venture partners, and relationships with politically exposed persons where the proposed business relationship involves, or is linked to, a prominent public official.

---


Depending on the company’s business, where it operates, and who it does business with, the risk assessment should be adjusted accordingly. This applies to all compliance areas. Furthermore, it is important to note that compliance risks can be exacerbated when the company has a complex supply chain and does not exercise effective control over it. A risk assessment should take into consideration the company’s supply chain, which includes direct and indirect suppliers. Responsible supply chain management is briefly described under paragraph 4.5.3 in relation to labour standards and human rights; however, supply chain management is also relevant to other compliance areas.

It is necessary to have a deep understanding of the company in order to conduct a risk assessment. The risk identification stage should include input from all areas of business within the company. If the company has an internal audit function, much of the information can be gathered from internal audit reports and discussing the company’s risks with the audit function. Furthermore, the compliance officer should consider both existing risks and potential risks. Predicting what risks the company may face in the future is a challenging task, and is often done via brainstorming with a team that possesses a solid understanding of the company and its risks.

After identifying the risks that the company faces, the second stage involves determining the likelihood of each risk occurring and its potential impact on the company. The likelihood of a risk materialising more often depends on business aspects such as how the company conducts its business. Other factors include, for example, the existence of written compliance policies and procedures, the culture of compliance in the company, whether there have previously been compliance failures or near misses, communication of compliance policies and procedures and related training. The impact of the risk materialising refers to the extent that the risk might affect the company, which can include financial, reputational, employee, customer, and operational impacts.

Upon determining the likelihood and impact of the identified risks, the risks can then be prioritised. This can be done using a risk matrix or a scale for example (a basic risk matrix is shown below in Figure 1). It is not possible for a company to address all risks at once and keep documentation for various processes of risk assessment; therefore prioritising the risks enables the company to address the most important risks first.

Once a company has a full understanding of the risks that it faces, the likelihood of each risk occurring and its estimated impact, it can then proceed with developing an effective compliance policy and related procedures. The risk assessment also illustrates to the relevant regulator that the company has tailored the compliance programme specifically to the company, and explains why some risks were prioritised before others.

The initial risk assessment should be supplemented by at least annual risk assessments, given that laws change, enforcement trends alter and the company itself can develop within a given year. Annual risk assessments will ensure that the company’s compliance programme is directing resources to the relevant risks that the company is facing at that time. It is also evidence that the company’s compliance programme is a living document.

<table>
<thead>
<tr>
<th>Impact</th>
<th>5</th>
<th>10</th>
<th>15</th>
<th>20</th>
<th>25</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>8</td>
<td>12</td>
<td>16</td>
<td>20</td>
<td>25</td>
</tr>
<tr>
<td>3</td>
<td>6</td>
<td>9</td>
<td>12</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>6</td>
<td>8</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td></td>
</tr>
</tbody>
</table>

Figure 1: Example of a basic risk matrix. The horizontal axis refers to the likelihood of the event happening and the vertical axis refers to the impact of the event.

2.2 Appoint responsibility for legal compliance

2.2.1 Primary responsibility

The primary responsibility for the company’s compliance programme should reside at the highest level of the company; the board of directors. The board of directors should provide the impetus and oversight to the compliance programme. Furthermore, it sets the tone from the top; communicating the important message that compliance is a central and integral part of the board’s policy and the company’s culture. A culture of compliance is essential to the company’s compliance programme’s success.

Furthermore, according to the ‘Recommendations on Corporate Governance’ for listed companies, the board is recommended to adopt policies for the company’s social responsibility, and consider joining national and international initiatives. The board of directors should consider the company’s social responsibility strategy in conjunction with its compliance programme, since these two areas complement each other.


10 Committee on Corporate Governance, ‘Recommendations on Corporate Governance’ (2014), recommendation 2.2.1.
2.2.2 Delegation to a committee
Some boards choose to designate the responsibility of overseeing compliance to a committee within the company, either a board-level committee or a regular committee.

The majority of companies in the U.S. for example, delegate the board of director's responsibility for compliance to the board's audit committee. However, in Denmark many companies do not have audit committees. The Recommendations on Good Governance recommend that for listed companies the board of directors set up a formal audit committee. Furthermore, the Committee recommends that the audit committee monitors and reports to the board on uncertainties and risks, prior to the approval of the annual report and other financial reports. Although the Recommendations are based on financial reporting, addressing financial risks and compliance risks complement each other, and thus the audit committee can play an important role in taking responsibility for the company’s compliance policy and procedures.

There is, however, growing international best practice whereby increasingly companies are choosing to establish a separate compliance committee at the board level, which is distinct from the audit committee. This development is likely to reach Denmark, and is particularly relevant for companies operating in highly regulated industries such as the pharmaceutical sector. With an increase in regulatory complexity, (large) companies are finding it more practical to create a compliance committee separate from the audit committee. Furthermore, establishing a separate compliance committee will ensure that compliance is afforded adequate resources, the committee has the relevant expertise to deal with specific issues of compliance, and the separation from the audit function will support the audit committee’s independence from the compliance function, thus allowing the audit committee to properly audit the compliance function.

Another option is for the company to designate responsibility for compliance to a non-board level committee. This can be a good alternative for non-listed smaller companies that do not have the capacity to set up separate board committees.

In any case, how the board of directors chooses to assign its responsibility depends on the company's size and the compliance risks that the company faces.

2.2.3 Responsibility for day-to-day operations
Upon establishing that the board of directors holds the primary responsibility for the company’s compliance programme, a responsibility that is sometimes delegated to a committee, a high-level individual should then be appointed with the responsibility to oversee and implement the company’s compliance programme (the ‘chief compliance officer’). In larger companies, often the chief compliance officer is separate from the compliance function so as to ensure independency and effective monitoring. The chief compliance officer should hold a position in the company that enables him/her to foster and promote compliance within the company. Depending on the size of the company and the industry it operates in, the chief compliance officer can be a part-time or full-time position with dedicated staff.

The chief compliance officer’s oversight and implementation of the compliance programme requires close coordination between the various activities that drive compliance. For example, the chief compliance officer should monitor the programme’s effectiveness in conjunction with internal audit, liaise with the legal counsel department, and ensure open communication with top management. The chief compliance officer should also ensure that new laws, regulations and renewed procedures are communicated to local compliance officers and country managers, ongoing training is provided, and compliance risks are monitored continuously.

The chief compliance officer should report, at a minimum, annually to the board of directors, or alternatively the relevant committee (e.g. audit committee), to give information on the implementation and effectiveness of the compliance and ethics programme. The chief compliance officer should also have access to the board of directors if needed, regardless of where he or she appears on the company organisation chart. In order to ensure that these reporting requirements are implemented, corporate compliance could be included as a subject to be discussed in the board of director’s annual wheel.

Overall, the governance structure of compliance should be tailored to fit the specific company. Responsibility for compliance can either be decentralised or centralised. An example of a decentralised approach is where the day-to-day responsibility for compliance is predominantly placed

12 Committee on Corporate Governance, 'Recommendations on Corporate Governance' (2014), recommendation 3.4.3.
13 Committee on Corporate Governance, 'Recommendations on Corporate Governance' (2014), recommendation 3.4.4.
14 See Committee on Corporate Governance, 'Recommendations on Corporate Governance' (2014), recommendation 2.1.1.
with the local managers; they are closest to the action and generally have a good understanding of the risks that the company faces, and can therefore monitor the implementation of the compliance programme and report back to the chief compliance officer. In comparison, a centralised approach builds in an additional layer of management into the company, which holds the day-to-day responsibility for compliance. The individual company will need to consider which approach is most suitable.

Below are two examples of how the compliance function’s governance structure can look for either a smaller company or a larger company:

*Small to medium sized companies can structure their compliance function for example:*

- **Board Of Directors**
  *(Primary responsibility)*

- **Compliance Committee/ Legal Department/ Risk Management Department**
  *(Optional – Board can delegate oversight responsibility)*

- **Compliance Officer**
  *(Responsible for day-to-day operations)*
  Example – CEO, CFO, in-house lawyer

- **Business Area Manager**
  *(Reports to Compliance Officer)*
Larger/publicly listed companies can structure their compliance function for example:

2.3 Establish standards and procedures
Following a comprehensive risk assessment and the appointment of responsibility for compliance, the company is at the stage to develop a compliance policy and procedures. The aim of establishing a compliance policy and procedures (‘compliance programme’) is to reduce the risk of compliance infringements. The compliance policy is the company’s overarching policy on compliance concerns, tailored specifically to the company’s culture and activities. Notably, it is becoming increasingly recognised that a compliance policy is best drafted in conjunction with the company’s ethics policy. Adopting this holistic approach increases the likelihood of the compliance programme to be effective, as the compliance programme should be based on a company culture of integrity and strong ethical values.\textsuperscript{15} The US Sentencing Guidelines also recognises this symmetry; it refers to ‘compliance and ethics program’.\textsuperscript{16}

The related compliance procedures can be drafted as a ‘code of conduct’ or as a manual. The code of conduct is the heart of the compliance programme. It is a manual designed to support day-to-day activities to be followed by the company’s employees and other company representatives, such as subcontractors, consultants and suppliers, who are at risk of violating compliance standards. Factors to consider when drafting a code of conduct include:

\begin{itemize}
  \item The code of conduct should be drafted in plain language, and consider using the local languages where the company operates.
  \item Avoid including burdensome references to laws and regulations.
  \item Include a short summary of the rules and their practical meaning.
  \item Draft the procedures proportionate to the risks that the company faces.
  \item Be succinct; avoid creating a long document that is unlikely to be read by the target audience.
  \item Tailor the code of conduct to the specific needs of the business units.
  \item Include practical examples, lists of ‘dos and don’ts’ and checklists.
  \item Highlight the potential costs of non-compliance.
  \item Include the relevant responsible person for compliance questions, and how to contact them if in need.
\end{itemize}

It may be necessary to create more than one code of conduct. Depending on the areas relevant for the company, a company may, for example, draft separate codes of conduct covering competition law, anti-corruption, export control and data protection. Furthermore, within the areas of risk, the company should consider the specific issues that employees and company representatives face. For instance, if a company is a dominant undertaking according to the EU Commission’s definition, then the code of conduct should provide specific guidance to employees on, for example, giving discounts. A dawn raid manual is also commonly included in a company’s compliance programme, so that staff are well informed on the procedure to follow in the case of an unannounced visit by the competition authority. It is critical that the code of conduct is tailored to the activities of the employees and company representatives and the specific risks they may encounter.


In addition to creating an overall compliance policy and code of conduct, it may also be necessary for the company to establish protocols on screening and monitoring business partners and third parties. Protocols can include background checks of business partners in high-risk areas, due diligence on third parties and business partners, incorporating strict compliance covenants in third party contracts, and auditing existing business parties. These procedures should also be outlined in the company’s policy and highlighted when concluding contracts with new business partners. The procedures must also be updated regularly.

The compliance programme will also need to include disciplinary procedures in case of non-compliance. The disciplinary action may differ depending on the conduct in question, the impact and whether an employee or third party was involved in the alleged infringement. It is important that such disciplinary procedures are included in employee contracts and contracts with third parties, so that they are enforceable.

Lastly, the compliance policy and procedures must be easily and readily available for employees and company representatives. Thought should be given to the means of publicising and distributing the compliance programme, for example whether it should be uploaded on the company’s intranet and/or distributed in paper format. These considerations will be covered in section 2.4 below, concerning implementation.

2.4 Implement
The implementation process is crucial to the success of the company’s compliance programme. Implementation requires both widespread communication of the compliance programme and proportionate training.

2.4.1 Communicate
The first step in implementing the compliance programme is to raise the level of awareness in the company on compliance in general: the compliance officer should publicise his or her role, what compliance is about, and that the compliance team is there to assist employees. Following this general introduction, the company must communicate its compliance programme effectively, both internally and externally.

The company should widely disseminate its compliance policy and code of conduct, and related guidance, to its employees in a format that is easily and readily accessible, and in a language that the employee can understand. Importantly, although it is not necessary for each employee to receive a hard copy of the compliance programme, all employees must be aware of the programme, know where to find a copy of the programme and who to direct questions to. A company should also consider requiring employees to sign a statement that they have received and understood the compliance policy and procedures. This could be done after training, for example.

It is also necessary for the company to communicate its compliance programme to contractors and other external partners, since such third parties fall under the company’s compliance risk profile. The company should be explicit in communicating to existing and potential business partners that it expects them to understand and comply with the compliance policy and procedures. To this extent, the company should include a compliance clause in the contractual framework. Furthermore, the company should communicate its compliance policy externally, via its website for example, in order to both reassure existing and prospective business partners of its stance, and to also act as a deterrent to those intending to breach its compliance policy on the company’s behalf.

Communicating the company’s compliance programme should be done periodically and in a timely manner, taking into consideration that the company’s compliance programme is regularly updated, and new employees and company representatives join the company. Periodic communication should also go hand-in-hand with the required training.

2.4.2 Training
A critical aspect to implementing the company’s compliance programme is to conduct appropriate training within the company. For the compliance programme to be effective, employees must be properly trained according to their exposure to risk. All employees should be aware of the compliance programme and be given basic training on the programme; however, some employees require more comprehensive training and should therefore be prioritised. Country managers and employees working in high risk areas should, for example, be given priority in the training; the company should first focus on the employees who can potentially create the most risk for the company, and then expand the training from there. Not all employees need the same type and the same level of training. For example, a sales employee with direct contact with government officials or with state-owned entities should be given specific training on anti-corruption laws, in addition to the more general compliance programme training. As another example, managers should receive comprehensive compliance training as they are best placed to help address risk by recognising and encouraging ethical behaviour by their subordinates. It is essential that the company tailors the training to the employee and the compliance risk in question, otherwise the training risks being ineffective.
Effective training should provide an overview of the company’s policies and procedures, a summary of the applicable laws, practical advice to address real-life scenarios, and incorporate case studies that apply the training. The training should also cover who the employee can contact when in (urgent) need of advice. What is important is that the employee is equipped with a sound understanding of what compliance is, the importance of compliance, the company’s compliance programme, how it applies to them, and what to do when faced with a compliance issue. Specific guidance concerning particular areas, such as what to do in the situation where a public authority arrives unannounced at the company to conduct a competition law investigation (a ‘dawn raid’), should also be considered. The company could, for example, conduct a mock dawn raid to train the receptionists, IT personnel and other relevant employees, on what to do in such an event.

Training can be conducted in various ways. In addition to more traditional mechanisms such as presentations and seminars, the company can utilise the numerous technological options available today, making training easier and more affordable for the company. The format and content of the training must be suited to the company’s employees. To ensure that employees have completed the training, attendance should be documented. In addition, to gauge whether employees understood the content of the training, they could be required to complete a survey or questionnaire. Positive incentives for completing compliance training could include explaining that the training is a way to advance an employee’s career.

Training should be conducted periodically. As the company’s compliance programme evolves, so too should the training programme. New employees need to be inducted with training on the compliance programme, and updates to the compliance programme must be communicated effectively, with the necessary training provided. Furthermore, the trainers should listen to the questions being asked and the feedback given during training: such communication will indicate the issues that are commonly faced by employees, which in future can be incorporated into the training programme.

2.5 Periodic review

‘A good compliance program should constantly evolve’. As the company changes and the environment in which it operates in changes, so too should the company’s compliance programme develop. It is therefore necessary to undertake periodic review of the compliance programme to evaluate its

---

effectiveness, and where necessary adapt it. Periodic review is facilitated by monitoring and auditing functions and reporting obligations.

2.5.1 Monitoring and auditing
A company should incorporate both regular monitoring and auditing functions to ensure that its compliance programme is an effective tool. Monitoring refers to regular reviewing and detecting compliance problems with a view to prevention, whereas auditing refers to a more limited review targeting a specific area, for example a business component, region or market sector during a particular timeframe, and is usually a reaction to a detected infringement.

To monitor the company’s compliance programme’s effectiveness, first consider monitoring whether individual behaviours within the company meet the compliance requirements. No matter how ‘strong’ a compliance programme may seem on paper, it will not be effective if employee behaviours are not aligned with the policy and procedures; employee behaviour carries the greatest risk for compliance control. Monitoring individual behaviours can be done via conducting staff surveys or questionnaires and receiving feedback from compliance training. It is also important to monitor whether managerial tasks that are designed to implement the compliance programme are in fact followed. Furthermore, reviewing information produced by internal/external auditors will provide a good overview of if the compliance programme is in fact effective. Lastly, consider the scope for benchmarking against commonly accepted ‘best practice’.

According to the ICC, undertaking an assessment of the programme should focus on three aspects: the compliance programme’s effectiveness (both design and operation); efficiency (the cost of the programme); and responsiveness (the programme’s ability to operate quickly and flexibly). Monitoring should be conducted regularly, with a thorough programme assessment conducted approximately every three to five years.

An audit may be necessary from time to time to investigate specific risk concerns, particularly after an infringement or suspected infringement surfaces. For example, a company based audit can be based on a list of payments made to suppliers over the last year, in order to detect corruption concerns. It is necessary to conduct audits promptly upon detecting an infringement, and often an audit will lead to a specific review of the compliance programme with a view to adapting the compliance programme so that an infringement does not occur again. Both monitoring and auditing serve the same purpose of continuously improving the compliance programme and ensuring its sustainability.

2.5.2 Reporting
Compliance reports should be sent to senior management at least annually, containing a description of the implementation and effectiveness of the company’s compliance programme. In order to realise this reporting requirement, as an example, country managers could be required to complete regular compliance reports submitted to the chief compliance officer. Furthermore, if the company has a legal department and an internal audit department, they could cooperate in monitoring the compliance programme’s effectiveness and reporting to senior management. In addition to regular reporting, where the compliance officer finds a significant compliance issue, the compliance officer should report this promptly to senior management. The compliance committee, or equivalent committee, should also receive the annual and periodic reports.

2.6 Handling concerns/Whistleblower system
An effective compliance programme must have a system or mechanism whereby employees can report concerns regarding compliance issues. This can be via informal means, for example where employees feel comfortable, they are encouraged to raise concerns with their supervisor. Such an informal approach requires the company’s compliance expectations and culture are understood by employees and managers, and that managers are also well-trained in the company’s compliance programme and understand their role in listening to compliance concerns, reporting such concerns and managing issues.

An informal approach is, however, insufficient on its own. A company should have an anonymous and confidential reporting system, such as a whistleblower hotline or webline, where employees can ask questions and report potential violations about ethics, company policies and compliance matters.

2.6.1 Whistleblower system
An effective whistleblower system, either a hotline or a webline, should be anonymous and confidential, and the whistleblower should not fear retaliation. The whistleblower system can be used to either report or seek guidance regarding potential or actual instances of non-compliance. It is important that the whistleblower system is publicised in a language that the employee can understand. Furthermore, there should be concrete guidance on why and when the whistleblower system should be used, and how to access it.

---

The whistleblower system can be administered either internally or externally, depending on the availability of resources. Note that there are potential conflicts of interest if administered internally and if a perception of bias is present then this may discourage potential whistleblowers. Larger/multinational companies should consider a global reporting system, administered externally, available to both employees and third parties, accessible 24/7 and offering various reporting avenues in a number of relevant languages.

Lastly, the whistleblower system should develop as the company’s compliance programme develops; it is an evolving system.

Under various jurisdictions, whistleblowers are afforded protection. For example, in the U.S., individuals who come forward and report possible violations of the federal securities laws to the Securities and Exchange Commission (SEC) are protected from retaliation by employers. Employers may not discharge, demote, suspend, harass or in any way discriminate against an employee who has lawfully provided information to the SEC under the whistleblower programme or assisted in any investigation or proceeding based on the information submitted. In the case of wrongful retaliation by an employer, the employee may bring a private action against the employer and the SEC can also take legal action in an enforcement proceeding against an employer who retaliates against a whistleblower. Whistleblowers are also incentivised with monetary rewards for individuals who come forward and report possible violations of the federal securities laws to the SEC. To date, the largest whistleblower reward given was USD 30 million in September 2014, to a whistleblower living in a foreign country.

It is important to note that due to the fact that the whistleblower system registers sensitive personal data, the company must notify the Danish Data Protection Agency (DDPA) and obtain authorisation prior to processing the data. The DDPA has developed guidelines for submitting notification of whistleblower systems.

2.6.2 Investigation
The company should respond promptly and fairly to concerns reported, either informally through a supervisor or formally via the whistleblower system. Non-existent or slow responses to compliance concerns will erode employee trust in the reporting system. Investigations can be conducted internally by the internal audit function or legal department. However, where the investigation concerns significant infractions or involves higher management, the board of directors should be informed and external counsel retained to avoid a conflict of interest. Reports should be kept confidential, and the company should consider personal data protection concerns. Importantly, the company should ensure that there is adequate protection for employees who report compliance breaches.

Overall, a whistleblower system is advisable; it is an additional support to encouraging a workplace environment whereby compliance concerns are raised and handled early, and employees do not fear retaliation.

2.6.3 The Mediation and Complaints-Handling Institution for Responsible Business Conduct
Companies should also note that Denmark has a ‘National Contact Point’ – The Mediation and Complaints-Handling Institution for Responsible Business Conduct – which deals with cases relating to non-compliance with the OECD Guidelines for Multinational Enterprises. The OECD Guidelines for Multinational Enterprises contain recommendations from the signatory governments (which includes Denmark) on responsible business conduct in areas such as employment and industrial relations, human rights, environment, information disclosure, combating bribery, consumer interests, science and technology, competition, and taxation.

If a company is the subject of a complaint, the company will be informed when the Mediation and Complaints-Handling Institution accepts the complaint for further consideration or rejects the complaint. The company has to option to seek access to the complaint by the Public Administration rules. Note that the Mediation and Complaints-Handling Institution determines whether the complaint is resolved, meaning that even if the company has come to an agreement with the complainant, it must be approved by the Mediation and Complaints-Handling Institution. To date, the Mediation and Complaints-Handling Institution has decided only one case.

2.7 External Reporting
Companies should also be aware that external reporting obligations, both financial and non-financial, can cover compliance risks and therefore reporting obligations should be considered when implementing a compliance programme.

-------------------------
20 Danish Act on Processing of Personal Data ss 48 and 50(1).
22 See their homepage at http://businessconduct.dk/home/0/2 for further information.
2.7.1 Financial Reporting

EU

Company reporting obligations primarily concern financial risks: legal compliance risks, or general risk management, are not usually covered under the scope of reporting obligations. According to the EU 2004 Transparency Directive, issuers must include a description of the principal risks and uncertainties that it faces in its annual and interim reports. Furthermore, the Fourth and Seventh company law directives requires companies to include 'a description of the main features of the company’s internal control and risk management systems in relation to the financial reporting process'.

In order to realise an efficient system for financial reporting, it makes business sense for the company to integrate internal controls regarding financial reporting into the general legal risk management system.

Denmark

Danish law requires listed companies to prepare a corporate governance statement indicating to what extent the company observes the Recommendations on Corporate Governance, following the 'comply or explain' model. The statement must include, among other things, a description of the main elements in the company’s internal control and risk management systems in connection with the financial reporting process. The description should cover the procedures or systems the company has established in connection with risk control, including how management continuously identifies and controls the risks for significant errors in the financial report, and the internal control systems established in the company to make sure that significant errors in the financial report are identified and corrected.

---

23 Directive (EC) 2004/109 on the harmonisation of transparency requirements in relation to information about issuers whose securities are admitted to trading on a regulated market and amending Directive 2001/34/EC, articles 4(2)(c) and 5.
25 Committee on Corporate Governance, ‘Recommendations on Corporate Governance’ (2013).
26 The Financial Statements Act s 107b(6). See also, ‘Recommendations on Corporate Governance’, recommendation 5.1.1.
2.7.2 Non-Financial Reporting

Internationally

If the company has committed itself to international voluntary initiatives, such as the UN Global Compact, then it will also need to report according to the initiative’s requirements. As an example, the UN Global Compact requires its participants to issue an annual Communication on Progress (COP) and a public disclosure to stakeholders on new progress regarding implementing the UN Global Compact. The specifics of the non-financial report will depend on which (if any) international voluntary initiatives the company has signed up to.

EU

Within the EU, there is now a new directive amending Directive 2013/34/EU as regards disclosure of non-financial and diversity information by certain large companies and groups (the ‘Directive’). The Directive came into force 20 days after it was officially published on 15 November 2014. Member States are required to implement the Directive into national law by 6 December 2016, and thus the Directive will apply to reporting in the calendar/financial year of 2017. Denmark will need to implement the Directive and reconcile the Directive with the current Danish non-financial reporting rules. If the Directive applies to a company then it could impact on a company’s reporting obligations, which includes reporting on compliance related risks.

The Directive only applies to companies which have an average number of employees exceeding 500 and a balance sheet total exceeding EUR 20 million or a net turnover of EUR 40 million. Companies falling under this definition will need to include in their management report information relating to environmental, social and employee matters, respect for human rights, anti-corruption and bribery matters, namely (i) a description of the Company’s policy on each of these areas; (ii) the results of these policies; and (iii) the risks related to these areas and how the company manages those risks. If the company does not have a policy on one or more of these areas, it shall provide an explanation as to why not. The method of reporting is left to the company to decide.

Although recognised as part of a wider movement to encourage greater CSR transparency, the Directive also captures compliance issues, such as anti-corruption and bribery. It is therefore pertinent that a company consider whether it falls under the Directive’s definition of a large undertaking which is subject to the reporting requirements, and accordingly coordinate the implementation of these reporting requirements with its compliance function.

Denmark

In Denmark, listed companies, state-owned companies, and companies that have a balance sheet total of at least DKK 143 million, net revenues of DKK 286 million, and an average of 250 full-time employees, are required to report on their CSR policies, pursuant to the Danish Financial Statements Act. Specifically, the company must disclose its CSR policies; how the company translates its CSR policies into action; and an evaluation of what has been achieved during the financial year concerning its CSR initiatives. If the company does not have any CSR policies, this must be reported. From 2012, companies must expressly address human rights and climate impact reduction as part of their CSR reporting.

Note that proposed amendments to the Danish Financial Statements Act are currently before Parliament. The amendments implement the EU Non-Financial Reporting Directive and increase the non-financial reporting requirements, affecting group D companies from the 2016 financial year and large group C companies from the 2018 financial year.

Again, if a company falls under the scope of the Danish Financial Statements Act, then it may need to consider coordinating its reporting obligations with its compliance function.

Even if a company takes all steps to implement a compliance programme, a breach in compliance may still occur. In such a situation, how the company reacts is critical.

31 Act 2008-12-27 nr. 1403 on the amendment of the Financial Statements Act.
32 Act 2008-12-27 nr. 1403 on the amendment of the Financial Statements Act s 1.
3.1 Receiving the allegation and determining a course of action

An allegation can come from various sources: internal discovery of possible violation, a victim, a whistleblower, a third party such as the media, or via a government inquiry. How the company manages the complaint will depend on who brings the allegation; a dawn raid for example will require a different reaction from the company as compared with an internal complaint.

All complaints must be taken seriously and responded to quickly and appropriately. It is essential that the company does not ignore complaints and responds swiftly; otherwise it risks increasing the company’s odds of government enforcement and even invoking board members’ personal liability. The company should undertake a preliminary assessment of the allegation, considering the credibility of the allegation, the seriousness of the allegation, and whether it warrants immediate action. The credibility of the allegation is key to determining what steps to take. The company should look at whether the complaint was anonymous, detailed, material, believable etc. When receiving an allegation and deciding on what course of action to take, it is vital that the company documents all decisions and actions taken.

Importantly, one of the first steps to take upon receiving a credible allegation is to ensure that the infringement is stopped at the earliest possible stage, if it has not already been stopped. Swift action will minimise the infringement and limit the company’s exposure. A compliance programme, which incorporates reporting mechanisms, will go some way to ensuring that compliance issues are detected and addressed early on.

The company will then need to consider whether or not to conduct an internal investigation and take appropriate follow-on measures.

3.2 Internal investigation

Upon receiving a credible allegation and conducting an initial investigation into the complaint, the company may decide to undertake an internal investigation in order to establish the facts of the matter and address any problems. There is no strict legal necessity to undertake an internal investigation, but it is a prudent way to investigate allegations in order to avoid

---

33 Members of the board of directors may find themselves personally liable in some jurisdictions. In the USA and Australia, for example, directors of companies are bound by duties of loyalty and reasonable care in fulfilling their role in overseeing the company’s operations. Failure to investigate reliable allegations of misconduct can amount to failing to act in the best interests of the company, thus breaching their directors’ duties and exposing them to civil liability.
liability, limit legal risks and possibly contribute to a more favourable end result. The company should consider carefully the advantages and disadvantages before embarking upon an internal investigation.

The arguments in favour of conducting an internal investigation include:

– The company secures better knowledge of the case and its implications.
– The company can assess the risk relating to the case.
– The company gains an understanding of the extent/how widespread the problem is.
– The company demonstrates a willingness to take responsibility.
– It may minimise reputational risk if the case is publicly known, or becomes publicly known.
– It can reduce the risk of action by public authorities, or temper such action.
– Forms the basis for a decision on self-reporting.
– Forms the basis for any internal decisions, e.g. disciplinary action against individual(s).
– Basis for assessment of remedial action/change of procedures.

There are, however, risks associated with conducting an internal investigation which the company should be aware of, including leaks of damaging information, mishandling or losing key evidence, and eventual ‘cover up’ if the investigation is too wide or too narrow.\(^{34}\) Be aware that in some jurisdictions the authorities do not look favourably upon internal investigations, as they see such investigations as tampering with the aim and role of public investigations. However, this is not usually the case in Denmark; internal investigations are generally not discouraged by the public authorities.

The key to conducting an internal investigation is to adequately scope and decide on an appropriate format, and to maintain control over the investigation so that the matter can be investigated internally without public authorities or the media becoming involved. There are several factors to consider before launching into an extensive internal investigation, including:

1. Define the scope and type of investigation.
   a. The goal of the investigation should be to find and address any possible illegal activity. Accordingly, the investigation should have appropriate breadth, proportionality and a clear timetable. Consider also the timing and the logistics of the internal investigations, paying particular attention to multi-jurisdictional issues.
   b. Decide who should have overall authority over the investigation (for example, the board of directors, audit committee, special committee, in-house legal counsel).
   c. Consider whether to use in-house legal counsel or external legal counsel, or similar, to conduct the investigation. The advantages of appointing external legal counsel include: the investigation is unbiased and objective, external legal counsel hold specific expertise in the area, it avoids a drain on internal resources, and information about the existence of the investigation is contained.
2. Draft a mandate for the investigation.
3. Possibility to cooperate with the relevant public authorities.
4. Implementing the investigation. Consider, for example, whether the investigators should have access to all material or whether there should be restrictions to such access, if the investigators should have the option to external help, such as a forensics team, etc.
5. Witness interviews and conversations with employees. There are many practical questions that should be answered before conducting interviews.
6. Specific issues such as personal data law, the duty of confidentiality, management of media and the press, etc.
7. Documenting all steps of the internal investigation and retaining such documentation.

The company should consider such practical matters before embarking upon an extensive internal investigation, and it is very important that the scope and type of investigation is defined as clearly as possible early on.

### 3.3 Self-reporting and other follow-on measures

At the conclusion of an internal investigation, the company must decide on how to proceed:

– Internal or external reports, including the decision to self-report to the authorities.

\(^{34}\) See for example the Kongsberg case: http://www.ganintegrity.com/index.php/kongsberg-corruption-charges/.
Disciplinary proceedings.
Dealing with third parties (termination, contact with auditors, regulators).
Considering compliance lessons, and drafting amendments to the compliance programme.
Any civil remedies.

The company should follow-through on investigations, even if the decision is to not report. If the company fails to take action in a timely manner, then it will risk being perceived as not being seriously committed to preventing and detecting compliance infringements.

3.3.1 Self-report
In Denmark there is no legal obligation to self-report; companies are under a legal obligation to stop the illegal activity. However, in some cases it may be prudent to self-report the compliance breach to the authorities. Factors to consider in making this decision are:

- The seriousness of the compliance breach.
- Whether the practice in question has stopped.
- Whether follow-up steps have been taken (e.g. disciplinary measures).
- The available leniency opportunities.
- Who is aware of the breach.
- Whether there is any government involvement.
- Multi-jurisdictional matters (e.g. the authorities inform each other).
- What are the contingent liabilities.
- The reputational risks.
- The CSR profile of the company.

In deciding to self-report, the company will then need to consider when to do so and how.

Self-reporting and general cooperation with the authorities can lead to significant reductions in fines. For example, the EU Commission’s leniency programme offers the first member of a cartel that blows the whistle full immunity from fines. Cooperation from other cartel members can result in a reduction in the fine of 50% and companies that cooperate in settlement agreements with the Commission will receive a reduction in fine of 10%.35

Another potential benefit to cooperating with the public authorities is that the public authorities may decide against commencing criminal investigations. In the case of Norsk Hydro in 2008, the company employed two law firms to conduct a private investigation into allegations of corruption in Libya in connection with the merger between Statoil ASA and Norsk Hydro ASA’s oil and gas division. Norsk Hydro decided to report to ØKOKRIM, the U.S. Department of Justice, and the U.S. Securities & Exchange Commission, and to fully cooperate with the authorities throughout the private investigation.36 The public authorities decided against opening criminal investigations.

3.3.2 Disciplinary measures
The company should also consider whether, and if so what, disciplinary measures of an employee are in order if a breach of the code of conduct is discovered.

3.3.3 Modifying the compliance programme
To prevent future similar violations occurring, the company should consider revising the compliance programme and making necessary modifications. An internal investigation can assist the company in determining where the weaknesses lie in the compliance programme.

35 Community Notice on Immunity from fines and reduction of fines in cartel cases, 8 December 2006, OJ C 298/17.
36 See Wiersholm and Shearman & Sterling’s report to Norsk Hydro ASA Board of Directors at http://www.hydro.com/upload/33521/Final%20Libya%20Investigation%20Report%202008-10-06.pdf.
Below is a brief overview of several areas that may be of relevance for a company in drafting its code of conduct. Competition law, anti-corruption, export control, data privacy, labour standards and human rights, and tax are generally the areas that companies commonly face compliance risks. There may also be additional areas relevant to the company; the code of conduct must to be tailored to the specific company.

4.1 Competition Law

Competition law is generally an area where companies place significant importance on implementing a compliance policy and programme. If a company is not aware of the law, it is probable that it could unknowingly breach the competition rules, and accordingly risk significant penalties and sanctions, including fines, actions for damages, blacklisting from participating in tenders, and even imprisonment.

4.1.1 Competition Law: Overview

The object of competition law is to promote efficient resource allocation in society through workable competition to the benefit of business and consumers, and in particular to increase consumer welfare. The applicable competition rules depend on where the company is operating. This overview is based on the EU competition rules; however, the main principles are generally applicable in other jurisdictions, for example Denmark.

Competition law contains two important prohibitions: a prohibition against anti-competitive agreements and a prohibition against abuse of a dominant position. These two rules are briefly explained below.

4.1.2 Anti-competitive Agreements

Companies are prohibited from engaging in anti-competitive agreements.\(^{37}\) This means that companies must not enter into agreements (or other concerted practices) which have as their object or effect the prevention, restriction or distortion of competition.

Examples of generally prohibited agreements include agreements between competitors in the form of:

- Price fixing.
- Reductions in capacity or output.
- Market or customer sharing.
- Bid rigging.

\(^{37}\) Treaty on the Functioning of the European Union, article 101.
Agreements between companies on different levels of the supply chain may also raise competition law concerns, for example:

- Resale price maintenance or minimum prices.
- Certain exclusive supply arrangements.
- Certain single branding arrangements.

Furthermore, the definition of ‘agreement’ is broad: an agreement does not need to be formally created as a contract, and can, for example, be an oral agreement or a gentlemen’s agreement. In fact, any exchange of information between competitors that increases market transparency and thus facilitates the possibility of coordination of market conduct may fall under the concept of an agreement or concerted practice. Competition law, in this respect, is concerned with effects rather than formalities.

The most serious infringement of the prohibition on anti-competitive agreements is participating in a cartel. Cartels are highly prioritised in all competition law authorities’ competition law enforcement and the penalties attached are severe.

### 4.1.3 Abuse of Dominant Position

Companies that enjoy a level of market power that enables them to behave largely independently of their competitors are considered dominant and therefore subject to specific restrictions to ensure that they do not abuse their position.\(^{38}\)

Determining whether a company assumes a dominant position is based on a number of factors which indicate whether the company in question faces sufficiently strong competitive pressure, thus acting as a constraint on the company’s pricing and other market conduct.

Many competition authorities adopt a general presumption of dominance in cases where the company in question has a stable market share of above 50 per cent.

There is no exhaustive definition on what constitutes abuse of dominance. Abuse can be exploitative, for example in the case of charging excessive (unreasonably high) prices and also in certain cases of product tying. Abuse can also be exclusionary, aiming to foreclose competitors from the market, for example by:

- Pricing below certain cost benchmarks (predatory pricing).
- Requiring exclusivity of a customer or supplier.

### 4.1.4 Specific Issues

There are a few areas that a company should pay particular attention to, when dealing with competitors.

**Competitor relationships**

A company should always be cautious when dealing with competitors. Although it is not illegal to enter into agreements with competitors, to meet with competitors, or to speak with competitors, close relationships that result in information exchange may give rise to competition law concerns.

Exchanging information with competitors may raise serious competition law concerns. Generally, information about current or future strategy on the market, including pricing strategies, must not be exchanged. Historical information is generally legal to exchange.

**Trade organisations**

Although it is not illegal to be a member of a trade organisation, the risk of intentional or unintentional coordination is present and competition authorities accordingly pay attention to the discussions that take place in the trade organisation and the information made available to its members. Participating in a trade organisation must be treated as the same as dealing with a competitor.

### 4.1.5 Infringement

Infringement of competition law risks serious consequences. Infringement of EU competition law can result in a fine of up to 10% of the overall annual turnover of the company.\(^{39}\) Fines can be significant, for example in 2008 Saint-Gobain was fined EUR 715 million (as reduced on appeal in 2014) for its involvement in a series of anti-competitive agreements and concerted practices in the car glass sector.\(^{40}\) More recently, in June 2014 the EU’s General Court upheld a fine on Intel

---

\(^{38}\) Treaty on the Functioning of the European Union, article 102.

\(^{39}\) Council Regulation (EC) 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty, article 23(2).

Corps of EUR 1.06 billion for the company's abuse of dominance. In some countries, infringement of competition law can also result in imprisonment of the persons responsible as well as personal fines.

Non-compliance with competition law can also result in broader implications: anti-competitive agreements are rendered null and void, customers and companies affected by anti-competitive conduct may claim damages, there can be significant reputational damage and loss of goodwill, the costs of defending a competition law claim can be considerable, and competition authorities will afford greater attention to the company in future. The costs deriving from reputational damage can be even greater than the fine: Hoffman-La Roche's serious loss of goodwill in the 1990s following the global vitamins cartel case resulted in the company being placed first on the 'Top 100 Corporate Criminals of the 1990s', a reputation which was difficult to overcome. Moreover, EU rules on public procurement provide the contracting authority with a possibility of excluding from a tender procedure a company that has engaged in serious infringements of competition law.

4.2 Anti-corruption

The numerous rules on anti-corruption, for example the Danish laws on anti-corruption, the UK Bribery Act 2010 and the American Foreign Corrupt Practices Act of 1977 (FCPA), have created a complex regulatory environment whereby companies must take comprehensive measures in order to ensure compliance with anti-corruption laws. In recent years, this necessity has been made all the more pertinent, with high fines and hefty imprisonment sentences now a reality for companies infringing anti-corruption laws. For example, in December 2014 French firm Alstom entered a deal with the US Department of Justice (DOJ) to pay a record fine of USD 772 million after pleading guilty to bribing officials in Indonesia, Saudi Arabia, Egypt and the Bahamas and falsifying its books and records. The DOJ has also announced charges against five individuals, including four corporate executives. In September 2014 GlaxoSmithKline's Chinese subsidiary was fined USD 490 million and the former head of China operations given a three year suspended sentence for bribery in Indonesia, Saudi Arabia, Egypt and the Bahamas and falsifying its books and records. The DOJ has also announced charges against five individuals, including four corporate executives.

It is important to note that foreign laws, in addition to the Danish laws, can also be relevant for a company. Foreign rules can affect, for example, the actions of subsidiaries abroad, acquisitions of foreign companies, the actions of agents and suppliers, and the hiring of US or UK citizens. Below is a general explanation of the law on anti-corruption, based on the Danish law and taking the more stringent standard as best practice where relevant.

4.2.1 Public Sector

It is a criminal offence to bribe public officials ('active bribery') and for public officials to accept a bribe ('passive bribery'). Bribing a public official is the undue granting, promising or offering of a gift or another privilege in order to induce the public official to do or fail to do something in relation to his/her official duties. There must be intent to induce the public official. Accepting a bribe includes the undue receipt, demand or acceptance of a gift or another privilege. It is unlawful for a public official to accept unlawful remuneration even when the party facilitating the remuneration did not intend to induce the public official (i.e. did not intend to bribe the public official).

The definition of public official includes persons holding public office or function (elected officials, government or municipal employees, persons holding an office with the national courts), persons in a similar public function or office in a foreign country (including state-owned companies in such other countries), and persons who exercise a public function or office in international organisations such as the EU, the European Council, NATO, OECD and the UN.

4.2.2 Private Sector

It is a criminal offence to offer a gift or other favour to a private individual with the intent that the receiver shall neglect his/her duties as trustee, i.e. as employee, manager, director, representative, agent etc. Likewise, it is an offence to accept such a gift or benefit. The decisive factor is whether it is the intention that the receiver, in return for re-
ceiving the gift or favour, shall carry out any act or omission to act in a manner that is in breach of his or her duties.

A legal entity can be held liable for the act of individuals if the offence has a natural connection with the legal entity’s activities; the legal entity is not liable for individuals who act in furtherance of private interests.\(^{49}\)

4.2.3 Specific Issues

Facilitation payments, sometimes called ‘grease payments’, are small sums of money for facilitating routine administrative processes, and they are generally illegal. There are a few narrow exceptions depending on which law applies, but best practice is to have a company policy and culture of not giving facilitation payments.

Gifts and hospitality are also grey areas, for example giving gifts to public officials for special occasions such as birthdays, anniversaries and retirement. Best practice is that only reasonable and proportionate gifts and hospitality are allowed. The key is proportionality. Thus, for example, inviting a public official to attend a modestly priced dinner is unlikely to count as bribery, unless it could be seen as trying to induce the recipient to do or refrain from doing something in relation to his official function or duty.

Companies should also be aware that under the UK Bribery Act, a company falling under its jurisdiction will be liable to prosecution if a person associated with it bribes another person intending to obtain or retain business or an advantage in the conduct of business for that company. This provision has broad scope; a person is ‘associated’ with the company if he/she performs services for or on behalf of the company, which means that employees, subsidiaries, contractors, agents and suppliers could fall under its scope. The company will have a defence if it can prove that it had adequate procedures designed to prevent persons associated with it from paying bribes.\(^{50}\)

4.2.4 Penalties

Depending on the jurisdiction, a finding of bribery can result in significant penalties. In Denmark, active and passive bribery in the public sector is sanctioned with a fine or imprisonment for a term not exceeding six years.\(^{51}\) Bribery in the private sector is penalised with a fine or imprisonment up to four years.\(^{52}\) Furthermore, the profit resulting from the bribe may be confiscated.

\(^{49}\) Danish Criminal Code ss 26 and 27.
\(^{50}\) UK Bribery Act (2010) ss 7 and 8.
\(^{51}\) Danish Criminal Code ss 122 og 144.
\(^{52}\) Danish Criminal Code s 299(2).
Under the UK Bribery Act, individuals found guilty of bribery can be penalised with up to ten years’ imprisonment and/or an unlimited fine. Companies found guilty of bribery can be penalised with an unlimited fine.

Under the FCPA, criminal penalties for each violation of the anti-bribery provisions for corporations and other business entities is a fine of up to USD 2 million, and for individuals (including officers, directors, stockholders, and agents of the company) a fine of up to USD 100,000 and imprisonment of up to five years. The DOJ and SEC can also pursue civil actions for anti-bribery violations; corporations and other business entities are subject to a civil penalty of up to USD 10,000 per violation, and individuals are subject to a civil penalty of USD 10,000 per violation which may not be paid by their employer or principal. These fines, in combination with the penalties associated with breaches of the accounting provisions, create a complex system whereby the consequences of violating the FCPA can be significant.

4.2.5 Jurisdiction
The jurisdiction of anti-corruption laws varies, and can be quite extensive. The Danish laws on anti-corruption apply to actions and omissions that occur in Danish territory or on board Danish vessels. Actions occurring outside of Danish territory fall under the Criminal Code when the action is carried out by a Danish national or Danish resident and either the act or omission is criminal in the country where it took place, or both the perpetrator and the person who the act is directed against are Danish nationals or residents.

Danish companies can fall under the UK Bribery Act’s jurisdiction if the offence takes place in the UK or the act or omission would have amounted to an offence if it had occurred in the UK and the company has a close connection with the UK. However, the key provision on corporate liability is section 7; Danish companies can fall under UK jurisdiction if persons associated with the company bribe another person intending to obtain or retain business or a business advantage for the company. Danish companies can also fall under the FCPA’s jurisdiction if the bribery takes place in the US or the foreign bribery has a connection to the US (which is interpreted very broadly). It is therefore plausible that a Danish company’s action could be caught under the UK Bribery Act or the FCPA and possibly other jurisdictions.

4.3 Export Control
Companies within the EU territory active in exports must pay careful attention to the export control rules, which are based on EU regulations. Exports outside of the EU territory are covered by the general export control rules. In addition to the general export control rules, certain and specific jurisdictions are subject to further controls and restrictions imposed by the UN or the EU (‘sanctions’). Within the EU, exports can also be covered by certain rules.

If the export falls under the scope of the general export control rules, the exporting company must check to see whether it should notify or obtain authorisation from the Danish Business Authority, or otherwise risk facing criminal liability.

This chapter is based on EU export control rules. However, companies engaged in exports must also follow detailed local rules, for example, in the US. The US export control system is exceptionally complex, and therefore will not be covered in this guide.

4.3.1 Export Control: Overview
The purpose of export control regime is to ensure that products that can be used in the development of nuclear, chemical or biological weapons (weapons of mass destruction, or ‘WMD’) cannot reach military-related customers in critical countries. The export control rules do not just cover physical products, but also critical know-how and software. Export controls cover: (1) the export of products that can be used for both civil and military purposes (‘dual-use items’); (2) the export of products not covered by the dual-use items list but falling under the catch-all provisions; and (3) exports to particular countries and/or individual persons or entities falling under UN/EU sanctions.

When considering whether the export is a critical export and requires authorisation or notification, the company should generally look at these factors:

- Is the product contained in the EU control list on dual-use products? Or could the product nevertheless fall under the catch-all provisions because the product could be used in connection with WMD or military use in a country under an arms embargo?

---

– Is the export destination a critical country, for example Iran, North Korea or Russia?
– Are there unusual circumstances in relation to the customer or the use of the product, raising warning signs?
– Who is the end-user? Are there restrictions of payments to/from certain countries and persons?

4.3.2 Dual-Use
Dual-use items are products which can be used for both civilian and military purposes. The EU has established a control list of dual-use items ('EU control list'), whereby all items contained in the list are subject to export control and must be authorised prior to export out of the EU.\textsuperscript{60}
It is important to note that the control list is amended from time to time and companies must keep up-to-date with changes to the export control rules. A new control list has recently entered into force on 30 December 2014.

A company intending to export a product falling under the dual-use list must seek authorisation from the Danish Business Authority first.

Transfers within the EU of dual-use items contained in Annex IV \textsuperscript{61} require prior authorisation from the Danish Business Authority. Annex IV dual-use items are not as extensive as those listed under Annex I, but are particularly sensitive items.

4.3.3 Catch-All
Even if a product does not fall under the EU control list, it may be covered by the catch-all provision, which acts as a safety net. Products which are, or may be intended in their entirety or in part, for use in connection with WMD, or in violation of an international arms embargo, are also subject to the export control regime.

The company exporting the product should consider what the prospective end-use of the product is, in the hands of the specific end-user, when determining whether to apply for export authorisation. Accordingly, the exporting company must collect information to this effect. If the exporter is unsure, and has reason to believe that the product could be caught under this provision, then it should seek advice from the Danish Business Authority.

4.3.4 Sanctions
The UN and the EU have in place sanctions against countries and/or individual persons or groups, generally as a reaction to the country or person persistently violating international conventions and agreements, for example human rights. Sanctions can include among others a weapons embargo, entry ban, imposition of freezing of funds and economic resources, and further restrictions or bans on import and export of products.

Countries especially critical and subject to extensive sanctions include Iran, North Korea, Syria and Russia. All persons, groups, legal entities, bodies etc. subject to EU financial sanctions are listed on the EU Commission’s database, which is updated regularly.\textsuperscript{62}

A company intending to deal with a country, person or group that is subject to EU sanctions must exercise caution and check that the intended business is not under the scope of the sanction.

4.3.5 Authorisation
To receive export authorisation for products subject to export control, the exporter must apply to the Danish Business Authority for approval. There are three types of authorisations:\textsuperscript{63}

(a) Individual: For non-recurring export orders, exports to critical countries and critical end-users, and for authorisations in connection with the catch-all provision.

(b) EU General: For exports of EU control list items to the seven closely related countries (Australia, Canada, Japan, New Zealand, Norway, Switzerland, USA). However, critical products and some special products may not be authorised under the community general export authorisation.

(c) Global: For regular less critical exports of specific products for civilian end users in specific countries. A company exporting to its subsidiary outside of the EU can for example apply for this type of authorisation. The authorisation is valid for two years.

4.3.6 Penalties
It is the exporting company’s responsibility to establish whether its products for export are covered by the export control provisions and accordingly require notification or authorisation from the Danish Business Authority. Any breach of the export control regime is regarded

\textsuperscript{62} To access the database see http://eeas.europa.eu/cfsp/sanctions/index_en.htm.
as a criminal offence and is punishable by a fine or imprisonment for up to two years, and in aggravating circumstances up to six years.\textsuperscript{44}

4.3.7 Responsibility
A company engaging in exports must have a compliance programme in place in order to ensure that there are adequate procedures covering the export of critical products or exports caught by the UN/EU sanctions. If no such procedures exist, it is very difficult for a company to determine or catch compliance issues, thus risking criminal liability.

The compliance programme should specifically include the sales departments and finance department, as they are closest placed to the company’s business in exports. Since export control rules, such as the lists on controlled products and the sanctioned countries and individuals, are frequently updated, it is of utmost importance to ensure that the compliance programme is regularly updated and the sales departments and finance department are promptly informed and adequately trained.

Furthermore, due to the fact that the list of controlled products and sanctioned countries and individuals change frequently, it is advisable that the company protect itself contractually when making sales that involve exports outside of the EU territory.

4.4 Data Privacy
The complex and increasingly demanding regulatory environment concerning data privacy means that companies are required more than ever to ensure that they handle personal data in a manner compliant with the law. Currently the issue of data privacy is gaining even more attention; a new EU regulation has been proposed that will harmonise data privacy laws across the EU Member States.\textsuperscript{45} The proposed regulation is a comprehensive reform to the current EU data protection rules\textsuperscript{46} and it will have broad application with significant obligations placed on companies. If a company does not already have a data privacy compliance programme in place, then it is highly recommended that it consider doing so, and furthermore, existing compliance programmes will need to be amended if the proposed regulation comes into force.

\textsuperscript{44} Danish Business Authority Executive Order No. 475 of 14 June 2005 on exports of dual-use products and technologies.
\textsuperscript{45} Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) COM(2012) 11 final.
\textsuperscript{46} Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. The Danish law implementing the is Directive is the Danish Act on Processing of Personal Data.
4.4.1 Data privacy in Denmark: Overview
The Danish Act on Processing of Personal Data (the ‘Act’) applies to public and private companies that process personal data wholly or partly by automatic means, or by other means which form part of a filing system.\(^{67}\) Personal data is defined as any information relating to an identified or identifiable natural person. The company that is responsible for determining the purposes and means of processing personal data (the ‘controller’) must ensure that it is in compliance with the law, including compliance by all external or internal ‘processor(s)’ (the company(ies) that processes the personal data on behalf of the controller). A company with entities (e.g. affiliated companies or sister companies) in several EU/EEA countries and/or third countries may have to comply with multiple jurisdictions’ rules on data privacy.

The Act is applicable to controllers that are:
- Established in Denmark and the activities take place within the EU.\(^{68}\)
- Established in a third country and the processing of data is carried out with the use of equipment situated in Denmark.\(^{69}\)
- Established in a third country and the collection of data in Denmark takes place for the purpose of processing in a third country.\(^{70}\)

If a company falls under the definition of controller and is covered by the scope of the Act, as noted above, then it will need to introduce data privacy compliance procedures.

4.4.2 Rules on processing
Overall, data must be processed in accordance with good practice. The standards for good processing practice requires that data must only be collected for specified, explicit and legitimate purposes and further processing must not be incompatible with these purposes. Furthermore, the data must be adequate, relevant and not excessive in relation to the purposes.

The controller must, as a main rule, ensure that the data subject has given his/her explicit consent to the processing of his/her personal data.\(^{71}\) Such consent should be freely given, and should be a specific and informed indication of the data subject’s wishes whereby the data subject signifies his/her agreement to personal data relating to him/her being processed. Notification of the processing to the Danish Data Protection Authority (DDPA) may also be required, and is almost always required for employers.

Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or data concerning health or sex life, are deemed sensitive data and subject to specific provisions.\(^{72}\) Processing of sensitive data must not take place without approval from the DDPA, subject to few exceptions. Whether approval from the DDPA is required should always be assessed on the basis of the specific data processed for the specific purposes and how the flow of data takes place within the company group.

Notwithstanding the above, personal data may be processed without the data subject’s consent if specific circumstances apply and these circumstances justify processing without consent. For example, some processing of customer data or employee’s data is allowed without consent, but may require notification to the DDPA. However, a case-by-case assessment should always be undertaken.

4.4.3 Data subject rights
The Act also provides data subjects with a number of rights.\(^{73}\) The controller must therefore implement internal and external policies which ensure that the relevant information is given to the data subject. For example, where a company’s website has an option for natural persons to enter their details, for instance to receive a regular newsletter via email, then the company will need to ensure that the person has given his/her explicit consent to the processing of his personal data and is informed of his/her rights in this regard.

4.4.4 Issues
Overview of data flows
To obtain an overview of the company’s current data flows and the level of protection afforded, the company should create a general control table and a database control table. The general control table relates to the overall personal data protection procedures that are in place throughout the entire business, including subsidiaries for example. The database control table relates to the contents of each database, including what type of personal information the database includes and what procedures are in place to handle the processing of such personal information. There should be a separate database control table for each separate

\(^{67}\) Danish Act on Processing of Personal Data s 3.
\(^{68}\) Danish Act on Processing of Personal Data s 4(1).
\(^{69}\) Danish Act on Processing of Personal Data s 4(3)(1).
\(^{70}\) Danish Act on Processing of Personal Data s 4(3)(2).
\(^{71}\) Danish Act on Processing of Personal Data s 6.
\(^{72}\) Danish Act on Processing of Personal Data ss 7(1) and 8.
\(^{73}\) See for example Danish Act on Processing of Personal Data ss 28, 31 and 35.
database in the company that holds personal information, typically a customer register, an employee register and a supplier register.

The database control table is a work tool for the company to obtain a general overview of the data flows in the company. However, there may be situations whereby the company requires specific assistance, whereby it is recommended to seek legal advice.

*Processing agreements*

When a company (the controller) utilises other parties for processing data, for example for storage of data or transfer of data, the company will enter into a processing agreement with the data processor. It is important that the roles of the processor and the controller are clearly defined and the responsibilities for each role are understood by each party. The legal obligations differ depending on whether the company is a controller or a processor of personal data, and if they operate inside or outside of the EU. It is the controller’s responsibility to ensure that any processing on behalf of the controller is performed under the instructions of the controller in compliance with the applicable law.

*Whistleblower systems*

Companies that have a whistleblower system in place must ensure that it complies with the data protection rules. In Denmark, companies must notify the DDPA prior to processing personal data obtained pursuant to a whistleblower system. There are guidelines from the DDPA on how to submit notifications concerning personal data obtained under whistleblower systems.

*Transferring data to a third country*

Personal data may only be transferred to a third country (a country outside of the EU/EEA) if the country ensures an adequate level of protection. Whether that country fulfils adequate level of protection requirement will depend on the circumstances of the case. Regarding transfers of personal data to the U.S., a special programme has been instituted (the ‘Safe Harbour Programme’) whereby the companies that have joined this programme are considered to have an adequate level of protection.

*Data retention*

In general, data must not be kept for a period longer than is necessary for the purposes for which the data are processed. Note that depending on the type of data collected, the retention time will vary. For example under the Danish Bookkeepers Act, accounting records must be stored for five years.

**4.4.5 Sanctions**

The DDPA is responsible for supervising all processing operations covered by the Act.

In the event of a breach, the controller is liable to a fine or imprisonment of up to four months, and should compensate the data subject for any damage caused. In general, the level of fines in Denmark is low, approximately between DKK 5,000 – 50,000. In 2001, daily paper Aktuelt was fined DKK 25,000 for breaching the Act’s procedures relating to the marketing of newspaper Politiken to Aktuelt’s subscribers, together with the transmission of Aktuelt’s customer register to Politiken.

It should be noted that all cases investigated and decided by the DDPA are made public on its website. Therefore a case on violation of the Act may result in damage to the company’s public reputation and recognition.

Companies should take note that the current EU proposed regulation introduces significant sanctions: fines of up to 5% of the company’s annual worldwide turnover or EUR 1 million for persons found responsible for breaching the relevant provisions. If the proposed regulation is passed, which is very likely, these sanctions are a significant increase on the current penalties for breaching data privacy laws. It will be of upmost importance for companies to prioritise creating data privacy compliance procedures in order to avoid falling foul of the new law and potentially becoming liable to pay a significant fine.

---

74 Danish Act on Processing of Personal Data s 48 and 50(1).
75 See http://www.datatilsy.net.dk/english/whistleblower-systems/whistleblower-guidelines/.
61 Danish Act on Processing of Personal Data s 27.
4.5 Labour standards and human rights
Within Denmark, if a company is complying with Danish employment and labour law then compliance with international labour standards is generally not an issue. Compliance issues usually surface when a company’s business activities span outside of Denmark and its operations are subject to lower, or even non-existent, labour and human rights standards.

4.5.1 International standards on labour
International standards on labour set out the basic principles and rights at work. The eight core ILO conventions outline the fundamental principles and rights at work, covering the areas of:

- Freedom of association and the effective recognition of the right to collective bargaining.
- The elimination of all forms of forced or compulsory labour.
- The effective abolition of child labour.
- The elimination of discrimination in respect of employment and occupation.

Denmark has ratified each of the eight fundamental ILO conventions. In addition to these fundamental principles and rights at work, the ILO standards also cover the areas including:

- Wages
- Working time
- Occupational safety and health
- Employment policy
- Employment security
- Social security
- Maternity protection
- Migrant workers

4.5.2 Supply chain management
Problems with labour standards and human rights compliance can occur when a company conducts part or the whole of its business outside of Denmark, particularly in developing countries. Issues can be exacerbated when the company has a complex supply chain and does not exercise effective control over it. It is predominantly the issue of supply chain management where companies should exercise care and implement a compliance programme.

According to the Danish Ethical Trading Initiative (DIEH), breach of international labour and human rights principles can be as a result of several factors:

- Local authorities
  - Gaps in the local law
  - Weak institutional capacity to implement and enforce the law
  - Competition for foreign capital

- Factory management
  - Competition for customers
  - Lack of knowledge regarding labour laws
  - Policy (e.g. to prohibit employee participation in unions)
  - Production planning and control

- Employees
  - Lack of knowledge regarding their own rights
  - Weak or lack of dialogue (for example through unions)

- Western importing companies
  - Irresponsible buying practices – price and time pressures, “diffuse” orders, lack of emphasis on good working conditions and environment

As an example, a company may foster breaches of international labour standards if it requires tight time pressures which make it necessary for a factory to force its employees to work without breaks.

83 See Freedom of Association and Protection of the Right to Organise Convention, 1948 (No. 87); Right to Organise and Collective Bargaining Convention, 1949 (No. 98); Forced Labour Convention, 1930 (No. 29); Abolition of Forced Labour Convention, 1957 (No. 105); Minimum Age Convention, 1973 (No. 138); Worst Forms of Child Labour Convention, 1999 (No. 182); Equal Remuneration Convention, 1951 (No. 100); Discrimination (Employment and Occupation) Convention, 1958 (No. 111).
The business case in favour of exercising responsible supplier management is strong:86

- Risks are better anticipated and managed.
- Operational risks, such as disruption to supply, are reduced.
- Improved working conditions can reduce turnover and improve quality and reliability.
- Costs are reduced and efficiency and productivity is enhanced.
- The company’s brand and value increases, alongside enhanced customer and consumer loyalty.

To exercise responsible supplier management a company should implement a compliance programme, following the guidelines outlined in chapter 2 of this guide. Note that responsible supply chain management is relevant to compliance issues additional to labour standards and human rights, for example anti-corruption and the environment. Importantly, even if a company is complying with the laws of the country in which it is operating, it is highly recommended that the company follow best-practice, choosing the higher standard where there is a conflict between the local law and best practice.

Specific Issues

Responsible supply chain management can be a complex and challenging task. How the company handles its sourcing responsibly also depends on whether the company is dealing with a direct supplier (for example through its supply chain) or an indirect supplier (for example through an intermediary). A company has a special obligation to its immediate suppliers, as the company holds a direct contractual relationship with them. A company can also influence its sub-suppliers, depending on its sphere of influence.

Responsible supply chain management essentially concerns the dialogue that companies create with the suppliers in order to ensure that fundamental labour standards and human rights are respected. In addition to the points outlined above in chapter 2 on creating and implementing a compliance programme, the company should use its influence to create continuous improvements with its suppliers. If a company finds that a supplier is not being cooperative, instead of switching to a new supplier the company should strive to collaborate to improve standards with the existing supplier, in order to improve ethical practices in supply chains. Obviously a company’s sphere of influence largely depends on its size: small and medium sized companies do not have the same ability as larger companies to influence suppliers.87

4.5.3 Opportunities

Although companies are not legally required to exercise responsible supplier management, the business case argues strongly in favour of practising responsible supplier management. Possibly the most persuasive argument is that in order to remain competitive in a global market, Danish companies are having to differentiate themselves from other companies, and on this point Denmark holds a strong reputation for being a world-leader in sustainability and CSR. Danish companies incorporating social responsibility will add value to their reputation and brand.

Large Danish companies are progressively adopting best practice in this area and implementing responsible supplier management into their compliance programmes. Furthermore, it is becoming increasingly common that larger companies are requiring from their customers to have compliance policies and procedures in place, as a pre-requisite to doing business with them.88 Small and medium sized enterprises in Denmark therefore frequently have to implement compliance programmes in order to conduct business with large Danish companies and stay competitive. This is overall a positive development which has resulted in increasingly more Danish companies following best practice when it comes to labour standards and human rights in the supply chain.

4.6 Tax

There are several issues pertinent to a company when it comes to tax compliance, beyond the general legal requirement to comply with the relevant tax laws. These issues are briefly outlined below.

4.6.1 Tax policy

A company should draft a tax policy, which sets out its position on tax compliance and further details the company’s procedures implementing the policy. This tax policy should be approved by the board of directors. The Recommendations on Corporate Governance support a company policy on tax by recommending that the board of directors ensure there is ongoing dialogue between the company and its shareholders in order for the shareholders to gain relevant insight into the company’s

---

88 See for example http://www.csrkompasset.dk/erkl%C3%A6ring-introduktionstekst.
potential and policies. Developing a tax policy is part of good governance practice. The tax policy should be available on the company’s internet and updated accordingly.

4.6.2 Guidelines for dealing with the authorities
Dealing with the authorities, for example regarding tax audits, tax investigations and visits (both announced and unannounced) by the tax authorities, can be a demanding situation for a company. If a company and its employees are not prepared for tax audits it risks causing increased compliance scrutiny by the authorities. A company should have guidelines in place to ensure that there is consistency in the company’s communication with the tax authorities. The guidelines act as a manual: it is a step-by-step guide on how to approach tax audits and communicate with the tax authorities, addressing all practical matters. Once such a manual is created, the company should ensure that it is distributed and the relevant employees are trained appropriately.

4.6.3 Incorrect tax returns
In the situation where a company discovers at a later date that it has made an incorrect tax return, in some jurisdictions it may be required to amend the tax return. For example, an employee engaging in bribery will enter the bribe payment as a ‘commission’, and consequently the accounting department will unknowingly process the payment in the tax return and claim a tax deduction. If the company later discovers this bribe, then it may be the case that it should amend its previous tax returns. In Denmark, it is very unlikely that there is an obligation to correct a previous tax return, if the tax return was accurate to the best of the company’s knowledge at the time of filing the tax return. However, in other jurisdictions, for example Germany, then the company may be required to amend the previous tax return and accordingly repay the tax refund received from the bribe. A company should be aware of this possibility.

4.6.4 Corporate income tax
The Danish Tax Authority (SKAT) publishes tax information on their website about public and private limited companies, cooperatives, foundations and associations paying tax in Denmark. The information includes the company’s tax obligation, any losses from previous years the company has drawn from the year’s income, the estimated tax for the income year, the tax provision the company is liable to tax under, and whether the company is subject to the tonnage tax.

Since this information is public, a company may wish to consider how it is perceived by the public, in terms of being a responsible company that pays corporate tax. For those companies that make a loss in the financial year and accordingly their tax liability is significantly limited, their (low) payments of corporate tax may receive negative press attention and in some cases public backlash. For example Nestle attracted increased media attention for paying ‘only’ two million kroner in corporate tax for 2013. The company will need to be prepared to explain how it contributes to Danish society, for example highlighting the other taxes that it pays, such as VAT, energy tax and taxes on employee wages.

89 Recommendations on Corporate Governance (2014), recommendation 1.1.1.
90 See http://www.skat.dk/skattelister.
92 See for example Novo Nordisk’s opinion on the public tax list: Steffen Moses, ‘Novo Nordisk mener at skattelisterne tegner et forkert billede’ Børsen (5 December 2013).
Companies today operate in a complex regulatory environment, which can be further complicated if the company employs thousands of employees, has subsidiaries in other jurisdictions, conducts business with international partners and engages with suppliers from around the world. Even in the case of smaller companies, complying with the relevant laws and regulations can be demanding because several laws have a wide scope of application (for example the UK Bribery Act) and overall public authorities are increasing their enforcement efforts. With compliance ranking high in terms of risk to the company’s reputation, in addition to the severe consequences that can arise out of non-compliance, such as significant fines, civil damages and liability for the board and management, it is clear that companies should place compliance high on their agenda.

Despite this challenging environment, companies can take effective action. Upon recognising that compliance is important, a company can implement an effective compliance programme, according to the steps outlined earlier in this guide. It is important to remember that implementing compliance into a company is not merely a ‘tick-the-box’ exercise: the compliance programme should be tailored to the individual company. Moreover, the board should ensure that it sets the tone of compliance and fosters a culture of compliance within the company. A culture of compliance goes a long way towards ensuring that the company’s compliance programme is actually effective.

Developing a compliance programme and ensuring that it is effective can prove to be a difficult task, and it may be necessary to engage external legal advice. Law firms can assist companies, namely by:

- Conducting a risk assessment
- Developing a compliance programme, including the company’s compliance policy and related procedures
- Developing a whistleblower system
- Drafting codes of conduct for each relevant area of compliance for the company (e.g. competition law, anti-corruption, export control, data privacy, labour standards and human rights, and tax)
- Training relevant staff on the company’s compliance programme
- Conducting internal investigations in the case of a discovered or suspected breach
- Assisting in reporting discovered compliance breaches and cooperating with the authorities
Lastly, compliance is an ever-evolving topic, and the needs of the company regarding compliance are also fluid. Accordingly, it is good business practice for the board to annually consider the company’s position on compliance and set a strategy for the company.
How to get in touch

Gorrissen Federspiel | Copenhagen office
H.C. Andersens Boulevard 12
1553 Copenhagen V
Denmark
T +45 33 41 41 41 | F +45 33 41 41 33

- Our offices are located in the center of Copenhagen
- 20 minutes by car from Copenhagen Airport
- 5 minutes walk from Copenhagen Central Station or Vesterport Station
- Gorrissen Federspiel has limited free parking space available

Public parking a few minutes away at:
- Jernbanegade 1, 1608 Copenhagen V
- H. C. Andersens Boulevard 18, 1787 Copenhagen V
Gorrissen Federspiel | Aarhus office
Silkeborgvej 2
8000 Aarhus C
Denmark
T +45 86 20 75 00 | +45 86 20 75 99

– Our offices are located in near the center of Aarhus
– 60 minutes by car from Billund Airport
– 20 minutes walk from Aarhus Central Station
– Gorrissen Federspiel has limited free parking space available

Public parking just next to our offices at:
– Silkeborgvej 2, 8000 Aarhus

LinkedIn
Join us on LinkedIn for the latest updates and insight from our firm. We post news and events frequently.
www.linkedin.com/company/gorrissen-federspiel

Newsletters
Subscribe for our newsletters and stay updated on the most recent development within various areas of practice.
www.gorrissenfederspiel.com/news
Gorrissen Federspiel

H.C. Andersens Boulevard 12
1553 Copenhagen V
Denmark
T +45 33 41 41 41

Silkeborgvej 2
8000 Aarhus C
Denmark
T +45 86 20 75 00

www.gorrissenfederspiel.com