

How to do Compliance Risk Analysis

THE FEDERAL OFFICE OF ECONOMY AND EXPORT CONTROL PUBLISHED A MANUAL FOR CONDUCTING RISK ANALYSES ACCORDING TO THE GERMAN SUPPLY CHAIN ACT

Executive Summary

- Wednesday, the August 17th, 2022, the Federal Office of Economy and Export Control (Bundesamt fuer Ausfuhrkontrolle or BAFA) published a “manual for conducting risk analyses according to the new German Act on Corporate Due Diligence Obligations in Supply Chains (Lieferkettensorgfaltspflichtengesetz or LkSG)” with the title “*detect, weigh and prioritise risks*”
- On a total of 21 pages, practical guidance and advice is provided in a comprised form underlining the central role of Compliance Risk Analyses in the context of new company duties and for the entire due diligence process related to human rights and environmental protection
- Following international examples, this also expresses the expectations of the BAFA as a public enforcement agency that must follow a risk-based approach itself in the execution of its public office in regulating and enforcing the LkSG
- The risk-based approach will be specified for all companies obliged to the new act. From January 1st, 2023 companies with groupwide more than 3000 employees are directly obliged regardless of their business model and corporate form; from January 1st, 2024 companies with groupwide more than 1000 employees will also be in scope
- For the very first time, the LkSG governs the protection of human rights and the environment as a corporate obligation and prescribes certain risk management-, documentation- and transparency duties within the supply- or rather the *value* chain in which beyond the company’s own operations, direct suppliers and service providers are explicitly captured as well as indirect business partners within the “deeper” supply chain
- The new BAFA-manual details the duty for regularly (at least annually) conducting risk analyses as well as the duty to conduct risk analysis on special occasions either in the event of investments, transactions and cooperations or when gaining substantiated knowledge of a potential violation at direct or indirect suppliers or service providers
- The BAFA underlines that the term *risk* is no longer only to be defined from a corporation’s- or entrepreneur’s perspective. With the new German Act on Corporate Due Diligence Obligations in Supply Chains coming into effect, the interests of obliged companies and their employees are now equally important with those interests of employees within the supply chain and all those that could be affected in any way by the activities of a directly obliged company or companies within its supply chain
- In face of these minimum compliance management standards, companies in scope of the LkSG as well as their contractual business partners need to review whether their implemented compliance management systems (CMS) satisfy the requirements set out by the BAFA regarding risk management in general and the actual level of risk analysis proficiency in detail



Background

On the June 11th, 2021 the German parliament passed the government draft for the Act on Corporate Due Diligence Obligations in Supply Chains (LkSG). Following its main regulations, a corporate responsibility for respecting human rights and protecting the environment is introduced for the first time in Germany. These responsibilities apply not only to the company's own operations, but also for contractual business partners like direct suppliers.

The **supply chain**, as explicitly mentioned in the title of the act must be understood as a comprehensive **value chain** according to its content. In Sec. 2 V. LkSG, the legal definition extends to all corporate activities for manufacturing a product or providing a service – starting with the extraction of raw materials up the delivery to the customer. The substantiated knowledge of potential violations of human rights at *direct* suppliers also triggers responsibilities according to Sec. 3 I. No. 8, 9 III. LkSG.

Addressees according to Sec. 1 LkSG are, regardless of the legal form, all companies with headquarters or head offices, administrative head offices or statutory head offices in the Federal Republic of Germany and over 3000 domestic employees (from January 1st, 2024 over 1000 domestic employees), including all expatriate and temporary workers with terms over 6 months. The scope of application extends also to foreign companies of all legal forms that have domestic branch offices and more than 3000 inland employees.

The LkSG formulates a comprehensive catalogue of **human rights related prohibitions** with explicit reference to the list of international treaties¹ attached to the text. These include the prohibitions of child labour; slavery; forced labour; disrespecting work safety; discrimination with respect to age, ethnicity or religion; insufficient payment as well as violations of the right to organize and form unions. In contrast, the **environmental-related responsibilities** are referenced to multilateral explicitly mentioned international treaties. Consequently, the

¹ As for example in the case of child protection Art. 24 I. of the international convention of civil and political rights or the UN-convention III., Art. 10 Nr. 3 the international convention of economy, social and cultural rights or the UN-convention I., International Labour Organization (ILO)-convention No. 138, ILO-convention No. 182

² Minamata-convention 2017

production or usage of mercury² and persistent organic pollutants³ is prohibited. Furthermore, the handling, the im- and export as well as the trade with hazardous waste⁴ is ostracised.

The responsibilities entitled by the legislator as obligatory efforts include a strikingly precisely formulated, very comprehensive portfolio of diverse prevention-, control- and remediation measures.

These include:

- The implementation of an appropriate **risk management**
- The definition of an internal **function**, e.g. a **human rights officer**
- The execution of appropriate **risk analyses**⁵ on a regular basis as well as additionally on certain occasions
- The adoption of a **policy statement on the human rights strategy** by the company management
- The implementation of appropriate **prevention measures**; explicitly mentioned are **procurement strategies and -practices** as well as **trainings** that protect human rights
- risk-based **control measures**
- enforcement of the expectations through **contractual audit- and special termination rights** (according to specially stipulated "Compliance Clauses")
- annual **review of the effectiveness** of prevention measures as well as occasion-related reviews in the event of substantial changes such as related to strategy, new market entries, new products or the acquisition of companies
- implementation and operation of an appropriate internal **complaints procedure** – in essence a Whistleblowing System

³ POPs- or Stockholm-convention 2004

⁴ Basel convention 1989

⁵ Comp. Sec. 5 LkSG: the legal wording of the de lege feranda prescribed risk term extends to two whole Din-A4 pages, alone for one section, Sec. 3 LkSG!



- **remedial actions** for detected human rights violations, from developing a joint remediation-plan together with Tier-1 business partners to the **termination of business contacts** as means of last resort⁶
- continuous internal reporting- and documentation obligations, including the duty to annually publish a specific report on the company's website

The LkSG **sanctions** include a financial penalty of up to 50 000 Euro, double the usual amount in administrative enforcement proceedings.⁷ The **administrative fines** can be extremely high and range between 100 000 and 800 000 Euro. Companies with over 400 Million Euro annual global- or group revenue can be fined up until **2% of that revenue** averaged over the last three years. **Asset forfeiture**⁸ related to a misdemeanor and a record at the **competition register**⁹ are further potential legal sanctions. Furthermore, the special capacity to bring legal action defined in Sec. 11 LkSG must be highlighted that entitles labor unions and non-governmental organisations (NGOs) to commence legal proceedings.¹⁰

The Risk Analysis as a foundation

The BAFA performed their legal duty as of Sec. 20 LkSG for specification by publishing a manual for conducting risk analyses according to the LkSG titled “*Detect, weigh and prioritise risks*” in German language.¹¹

These guidelines' content is defining the basic requirements for risk analyses and follows long standing international best-practices in compliance management. The format as a manual resembles the well-known practices of formulating compliance management standards given by the US Department of Justice, the US Stock Exchange Supervisory Authority, the UK Serious Fraud Office as well as comparable Brazilian efforts.¹²

Taking into account the ongoing international legal developments in the last ten years towards partly diverging standards in supply chain acts reveals at least one converging theme which is the significance of risk analyses. Similar acts have been adopted in California in 2010, in the UK in 2015, in France in 2017, in the Netherlands 2019 or in Norway in 2021.¹³

⁶ Thus in Sec. 8 II. LkSG expressly required

⁷ Sec. 22 LkSG; Sec. 11 III. Verwaltungsvollstreckungsgesetz (VwVG)

⁸ Sec. 29a Ordnungswidrigkeitengesetz (OWiG)

⁹ Sec. 125 Gesetz gegen Wettbewerbsbeschränkungen (GWB)

¹⁰ See also our GSK update of 27.09.2021, available at: <https://www.gsk.de/de/das-neue-deutsche-sorgfaltspflichtengesetz/>

¹¹ Available at: https://www.bafa.de/SharedDocs/Pressemitteilungen/DE/Lieferketten/2022_06_handreichung.html

¹² Comp. US DoJ / SEC FCPA Resource Guide, 2. Edition, July 2020, available at: <https://www.justice.gov/criminal-fraud/fcpa-resource-guide/>; UK SFO Bribery Act Guidance, Revised in October 2012, available at: <https://www.sfo.gov.uk/publications/guidance-policy-and-procedures/bribery-act-guidance/#:~:text=Bribery%20Act%20guidance%20UK%20companies%20that%20do%20business,and%20distributors%20adhere%20to%20the%20same%20high%20standards>; Controladoria- Geral da Uniao GCU do Brasil Programa de Integridade -

Diretrizes para Empresas Privadas, September 2015, available at:

<https://de.scribd.com/document/319469062/Programa-de-Integridade-Diretrizes-Para-Empresas-Privadas>

¹³ California Transparency in Supply Chains Act, Senate Bill No. 657, available at: https://oag.ca.gov/sites/all/files/agweb/pdfs/cybersafety/sb_657_bill_ch556.pdf; UK Modern Slavery Act, 2015 c. 30, available at: <https://www.legislation.gov.uk/ukpga/2015/30/contents/enacted>; LOI n° 2017-399 du 27 mars 2017 relative au devoir de vigilance des sociétés mères et des entreprises donneuses d'ordre (1) (FR “Loi de Vigilance”), available at: <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000034290626/>; Child Labour Due Diligence Law, available at: https://www.eerstekamer.nl/behandeling/20170207/gewijzigd_voorstel_van_wet; Norwegian transparency act 18th of June 2021 Lov om virksomheters åpenhet og arbeid med grunnleggende menneskerettigheter og anstendige arbeidsforhold (åpenhetsloven), available at: <https://lovdata.no/dokument/NL/lov/2021-06-18-99>



In the meantime, since February 23rd, 2022 a proposal of the EU for a Directive on Corporate Sustainability Due Diligence has become available.¹⁴ It exceeds the regulations of the German Supply Chain Act in many points, especially its definition of risk sectors, the lower application thresholds in terms of employee numbers (500 in general or down to 150 in explicitly mentions high risk industry sectors such as textile, agriculture, wood, food, oil and gas) according to Art. 2., the explicit reference to the entire value chain in Art. 3 lit. g.), the unambiguous stipulation of a civil liability in Art. 22, the containment of climate change by following the 1,5°C threshold as an independent sustainability responsibility in Art. 15 and most of all the explicitly extended individual liability for all members of corporate management in Art. 25.¹⁵ The necessity for conducting risk analyses is formulated in Art. 6 as a corporate responsibility for detecting substantial as well as potential negative consequences on human rights and the environment.

In general, the converging basic pillar of a risk-based approach is again confirmed herewith. Consequently, it is of great importance if, as required by Sec. 4 I. LkSG, an appropriate and effective risk management is implemented whose core is the risk analysis as defined by Sec. 5 LkSG. In other words: without an appropriate risk analysis no appropriate weighing and therefore no plausible prioritisation of the human rights- and environmental risks for the company itself. The BAFA-manual stresses that the entire due diligence process – i.e. the prevention measures, the remediation steps, the complaints procedure and last but not least the reporting and documentation duties - is heavily depending on the actual quality of the preceding risk analysis. That will substantially influence the interpretation of the undefined legal term “appropriate” in Sec. 3 II. LkSG. The explicitly specified criteria regarding the form and extent of the actual corporate influence on the party directly responsible for causing a risk, the expected severity of the violations, their likelihood and reversibility as well as the nature of causal contribution are offering opportunities for companies on the one

hand side for developing a specific compliance management approach for themselves and to prioritise their scarce resources accordingly in an aptly targeted manner. On the other hand, the appropriateness criteria specified by the BAFA-manual in No. 4.1 is also setting the minimum standards for preparing and performing effective risk analyses.

Risk management in the interest of third parties

The BAFA-manual clarifies that risk analyses according to the LkSG are distinctively diverging from formerly known risk analysis approaches for the identification of impending financial costs or reputational damages for the company. In contrast to the well-known enterprise risk management (ERM) approaches for example, the focus is no longer limited on the probability and severity of a damage. The BAFA explicitly demands not less than a change of perspective in No. 3.3 of the manual. In future, human rights related and environmental risks according to Sec. 4 IV. LkSG must be analysed in view of the interests of all employees in a company’s own operation as well as of those employees along the entire value chain. And also, of all persons that are adversely affected by the business activities of a company in any other way along the supply chain.

Three types of risk analyses

Once again, the BAFA-manual emphasizes and highlights by practical examples that risk analyses cannot be a once-in-a-lifetime-project only. First of all, risk analyses according to Sec. 5 IV. LkSG are to be conducted regularly once a year at least. Furthermore, event-triggered risk analyses must be conducted, too. A legally defined event is for instance a change of business activities. An assumed significance in that sense can result from internal business decisions not only related M&A activities or new joint ventures but also by the explicitly listed development of new sourcing countries. An external factor of significance for the risk situation can result from information about natural catastrophes in certain regions or the, sadly not that abstract any longer, outbreak of hostilities or an outright

¹⁴ EU COM 2022/0051, *Proposal for a Directive on Corporate Sustainability Due Diligence*, available at: https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/AUTRES_INSTITUTIONS/COMM/COM/2022/04-28/COM_COM20220071_DE.pdf

¹⁵ See our GSK Update from 25.02.2022, available at: <https://www.gsk.de/de/zum-vorschlag-der-neuen-eu-nachhaltigkeitsrichtlinie/>



shooting war. And lastly, event-triggered risk analyses must be conducted without undue delay according to Sec. 9 III. LkSG when a company has gained substantiated knowledge of a potential violation even at indirect suppliers. That stresses once again that at its core and contrary to its title, the LkSG does not only comprise direct suppliers but calls for a systematic analysis of the entire value chain including indirect suppliers which is framed as the “deeper” supply chain in the BAFA-manual. It is important in this context to note the reference in Sec. 4 IV. 2. to Sec. 8 LkSG. Because the substantiated knowledge can for example also stem from carefully handling hints given through the required complaints procedure. This stresses compliance management in accordance with the new German Supply Chains Act must consistently follow a systemic and integrated approach. And that the term due diligence is no longer a mere transactional notion related to M&A- or business partner due diligence, but must be understood as a continuous corporate duty.

Conclusion

What are the lessons from the new BAFA-manual?

Naturally, in 21 highly compressed pages there cannot be concrete advice for all possible company- and risk situations. A simple “check-the-box” answer for the eternal question of “how to do compliance risk analysis?” regrettably is also not provided.

And still, this official paper published by the competent regulatory authority brings the, for an act in German language already respectably detailed and practice-oriented, legal wording to an even higher level of granularity. On the one hand this is clear guidance for companies, on the other hand it also raises the expectations for their level of risk analyses.

The BAFA unfortunately misses the chance in this all in all very helpful guidance to deliver the inevitable clarification that an effective protection of human rights and the environment must not only include the *supply chain* – that is “downstream” – but extends along the entire *value chain* including the “upstream” business partners such as distributors or other kind of labour mediators. On this important point the proposed EU Directive from February 23, 2022 is decisively less ambiguous by explicitly using the term value chain; the BAFA at least uses the new term of a “deeper” supply chain.

Definitely helpful are the risk analysis toolbox additions listed in the attachments of the manual for conceptualizing the appropriateness criteria as well as the comprehensive overview of contemporary international practice- and industry sector guidelines. For those companies that have never performed an appropriate risk analysis before there won't be much time left. Many of the (large) companies that are directly obliged from January 2023 have already started to calibrate their existing CMS in face of the new risk categories human rights and environment – and have also demanded their business partners along their respective value chains to do so. And eventually it must not be forgotten with respect to the central compliance topic risk analyses that not only the BAFA as the competent regulatory authority has a close eye on the actual corporate compliance management capabilities. Moreover, thanks to the special capacity to bring legal action, there will be NGOs that are fairly active in the context of human rights and the environment who have also read this manual carefully – which definitely deserves a hot reading tip in an even hotter summer.

Eric Mayer

Attorney-at-Law (Germany)
Munich office
eric.mayer@gsk.de

Dr. jur Joshua Blach

Lawyer (Univ.)
Munich office
joshua.blach@gsk.de

Jan Schröter

Engineer
Munich office
jan.schroeter@gsk.de



YOUR PERSPECTIVE.

[GSK.DE](https://www.gsk.de) | [GSK-LUX.COM](https://www.gsk-lux.com)

Copyright

GSK Stockmann – all rights reserved. The reproduction, duplication, circulation and/or the adaption of the content and the illustrations of this document as well as any other use is only permitted with the prior written consent of GSK Stockmann.

Disclaimer

This client briefing exclusively contains general information which is not suitable to be used in the specific circumstances of a certain situation. It is not the purpose of the client briefing to serve as the basis of a commercial or other decision of whatever nature. The client briefing does not qualify as advice or a binding offer to provide advice or information and it is not suitable as a substitute for personal advice. Any decision taken on the basis of the content of this client briefing or of parts thereof is at the exclusive risk of the user.

GSK Stockmann as well as the partners and employees mentioned in this client briefing do not give any guarantee nor do GSK Stockmann or any of its partners or employees assume any liability for whatever reason regarding the content of this client briefing. For that reason we recommend you to request personal advice.

www.gsk.de

GSK Stockmann

BERLIN

Mohrenstrasse 42
10117 Berlin
T +49 30 203907-0
F +49 30 203907-44
berlin@gsk.de

HEIDELBERG

Mittermaierstrasse 31
69115 Heidelberg
T +49 6221 4566-0
F +49 6221 4566-44
heidelberg@gsk.de

FRANKFURT / M.

Bockenheimer Landstr. 24
60323 Frankfurt am Main
T +49 69 710003-0
F +49 69 710003-144
frankfurt@gsk.de

MUNICH

Karl-Scharnagl-Ring 8
80539 Munich
T +49 89 288174-0
F +49 89 288174-44
muenchen@gsk.de

HAMBURG

Neuer Wall 69
20354 Hamburg
T +49 40 369703-0
F +49 40 369703-44
hamburg@gsk.de

LUXEMBOURG

GSK Stockmann SA
44, Avenue John F. Kennedy
L-1855 Luxembourg
T +352 271802-00
F +352 271802-11
luxembourg@gsk-lux.com



YOUR PERSPECTIVE.

GSK.DE | GSK-LUX.COM