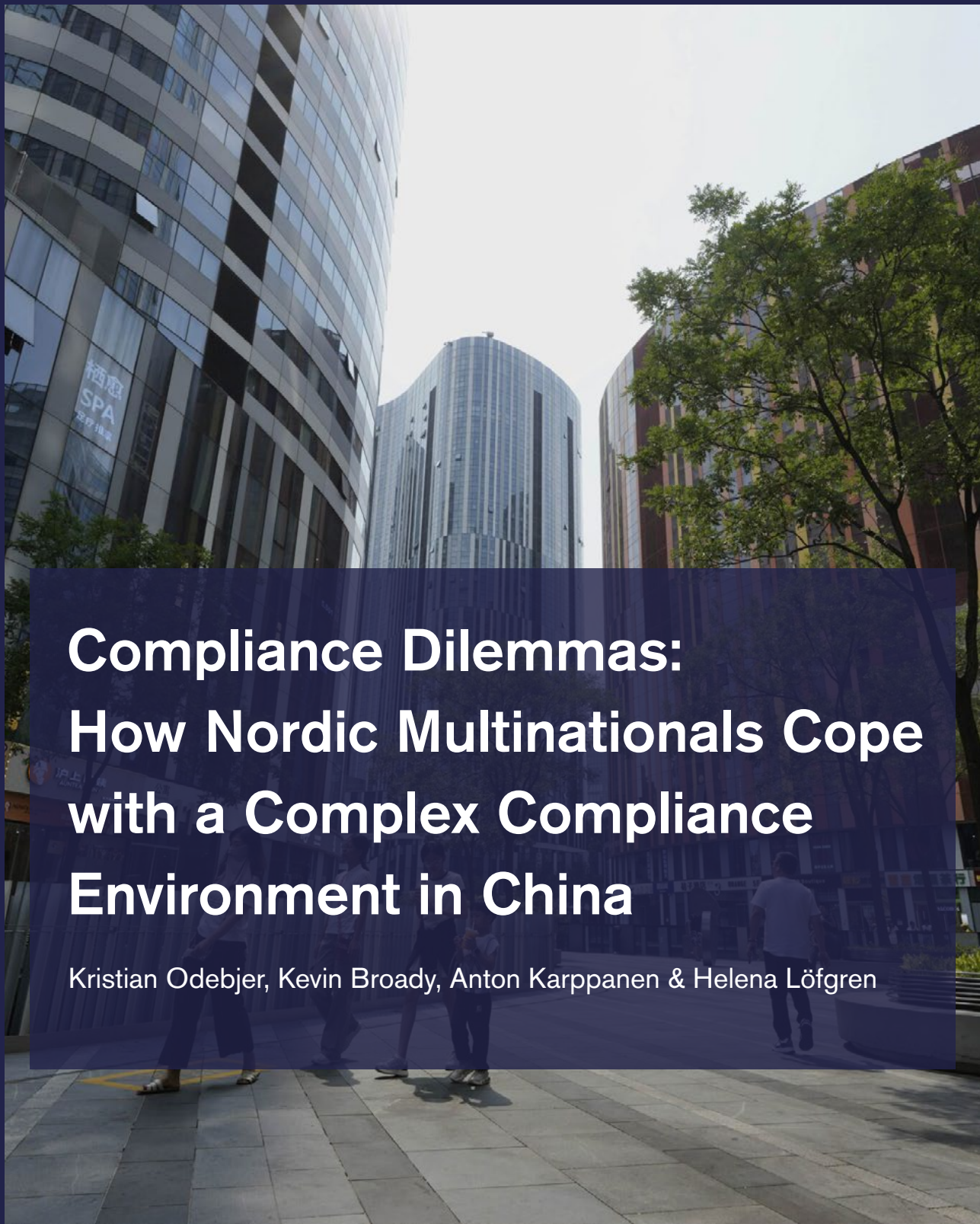


REPORT
NO. 4 2026

 **China Office**
of Finnish Industries

 **SWEDISH NATIONAL
CHINA CENTRE**



Compliance Dilemmas: How Nordic Multinationals Cope with a Complex Compliance Environment in China

Kristian Odebjer, Kevin Broady, Anton Karppanen & Helena Löfgren

Abstract

This study explores how Nordic multinational companies operating in the People's Republic of China manage difficult questions involving compliance with several legal regimes at once. It highlights how the environment has grown more complex in recent years due in part to geopolitical tensions. Typical risks are identified and a toolkit of “coping mechanisms” designed to manage these risks are introduced. The study contains recommendations for the worlds of business and government.

Contents

Foreword	4
Definitions, Acronyms and Abbreviations	5
Executive summary.....	6
1. Introduction.....	9
a. Objectives	9
b. Compliance Dilemmas	9
c. Methodology.....	15
d. Background: Business Sentiment and Compliance Challenges	16
2. Findings.....	18
a. Four Types of Compliance Dilemma	18
b. Pure Compliance Dilemmas	19
c. Home Country-driven Compliance Dilemmas	21
d. Host Country-driven Compliance Dilemmas: PRC data legislation.....	23
e. Code of Conduct-driven Compliance Dilemmas.....	26
3. Conclusions	30
a. Nordic MNC's experience of Compliance Dilemmas in the PRC.....	30
b. What strategies do Nordic MNCs in the PRC employ to cope with Compliance Dilemmas?	31
c. How significant is the impact of Compliance Dilemmas on the strategic objectives of Nordic MNCs?	33
4. Recommendations	35
Appendix A	38
Appendix B.....	44
Appendix C.....	47
Endnotes.....	48

Foreword

This study is the result of a pioneering collaboration between the Swedish National China Centre at the Swedish Institute of International Affairs and the China Office of Finnish Industries. It was initiated by Advokat Kristian Odebjer, a Swedish lawyer based in Hong Kong. The project team comprised Helena Löfgren, PhD, Analyst at the Swedish National China Centre; Kevin Broady, Chief Analyst at the China Office of Finnish Industries; Anton Karppanen, Analyst at the China Office of Finnish Industries; and Kristian Odebjer, Project Director.

The project team sensed that thorny compliance matters – or “compliance dilemmas” – were becoming of increasing concern to Nordic Multinational Companies (MNCs) operating in the People’s Republic of China and wanted to learn more about what this means for the day-to-day activities of those companies. In the light of the limited amount of existing research in the field, the team took advantage of the spirit of partnership that prevails in the Nordic community of PRC-focused business professionals, researchers and advisers.

Given the sensitive nature of the subject matter, we are very grateful to the participating companies for the unique insights they provided in the interviews that formed the core of the data collection exercise. We also wish to thank Dr Kelly Chen (Senior lecturer in private law at Södertörn University and Fellow in commercial law at Stockholm University) and Linda Jakobson (Board Member, China Office of Finnish Industries) who reviewed the report in draft and provided helpful feedback. Several other organisations active in the Nordic business community offered support along the way. Among them, the Sweden-China Trade Council and its Secretary General, Elisabet Söderström, deserve special mention. Our thanks also go to Dr Ji Li, Professor of US-China Business and Law at the University of California Irvine School of Law, who offered encouragement and guidance as the study was launched.

Since the study has two main audiences – the business and policy communities – some segments of the report may be more relevant to one audience than the other. Nonetheless, the project team hopes that the study as a whole will prove thought-provoking for both groups.

We believe that this study answers a number of important questions. It is clear, however, that it also raises new ones. Our recommendations therefore also touch on topics for further research. If you share our interest in learning about compliance dilemmas, please get in touch.

Hong Kong, Stockholm and Helsinki

September 2026

Advokat Kristian Odebjer

Boase Cohen & Collins

Björn Jerdén, Centre Director

Swedish National China Centre
at the Swedish Institute of
International Affairs

Kevin Broady, Chief Analyst

China Office of Finnish
Industries

Definitions, Acronyms and Abbreviations

CSDDD	EU Corporate Sustainability Due Diligence Directive
CSRD	EU Corporate Sustainability Reporting Directive
EU	European Union
Home Country	The home country jurisdiction of an MNC
Host Country	The host country jurisdiction where an MNC maintains activities
HQ	Headquarters
KYC	Know your customer checks, typically performed on the counterpart at the outset of a commercial relationship
MNC	Multinational company
PRC	People's Republic of China
SME	Small and Medium-sized Enterprises
UFLPA	US Uyghur Forced Labor Prevention Act

Executive summary

Nordic multinational companies (MNCs) operating in the People's Republic of China (PRC) face a structurally complex and increasingly fragmented compliance environment. Companies need to consider the overlapping and sometimes conflicting obligations that arise from Home Country (EU and national), Host Country (PRC) and Third Country (notably US) regulatory regimes, as well as internal Codes of Conduct. "Compliance dilemmas" have become a routine feature of operations rather than an exception. As a result, companies bear significant extra costs and shoulder risks that can have a severe impact on their ability to do business.

Compliance dilemmas are widespread but uneven in terms of their nature, severity of risk and degree of business impact. They vary by sector, supply chain complexity and organisational structure. While some dilemmas, such as sanctions screening, are already highly institutionalised within MNCs, others are ad hoc, context-specific and difficult to systematise.

While participants aim to detect sanctioned companies before agreements are concluded, these checks might fail: ***"It's always a risk-based approach and you can't really put a one-size fits all [solution] to fit the whole umbrella"***.

Participant in the study.

The prevailing international environment increases the risk posed by compliance dilemmas, as cross-border trade and investment are increasingly seen as potential threats to national security. Data and security legislation – be it Home Country, Host Country or Third Country – is a central and evolving source of compliance dilemmas, and sometimes causes "head-on" norm collisions (referred to as Pure Compliance Dilemmas in this study).

For example, a Nordic MNC that declines business with a sanctioned PRC customer may be charged with an offence under PRC Blocking Rules and related legislation. Nordic MNCs have so far assumed that the enforcement risk in this regard is relatively low, but this assumption will need to be continually assessed and potentially recalibrated as political tensions between the PRC and the rest of the world evolve.

Participants report that the PRC's ability to monitor international compliance is limited and ***"neither the PRC nor the EU has been great on extraterritoriality"***.

Participating compliance director.

Compliance dilemmas are a "design feature" of PRC legislation, as seen in the ambiguity inherent for example in laws covering foreign trade, supply chain scrutiny and data. PRC legislation relies on vague or evolving definitions, creating an operating environment that is characterised by extensive grey zones. The PRC authorities have wide discretion when enforcing these laws, which only amplifies uncertainty on the part of companies.

One informant highlighted the need to appreciate the practice of ***"selective enforcement"***, which implies that the participant's risk profile could increase as a result of external factors, such as sudden political developments involving the participant's Home Country.

Supply chain compliance is a core pressure point, where extensive foreign due diligence requirements meet practical and legal limitations in the PRC. Companies report that difficulties in verifying supplier information, an overreliance on self-certification and frequent constraints on site access contribute to their compliance challenges. Transparency at a level envisaged by emerging regulations, and often also expected by customers, might be difficult or even impossible to accomplish in practice.

"While the PRC may have its own challenges in some areas, their concerns with respect to sustainability reporting and due diligence were for the most part not unique to the PRC. [...]"

"The CSDDD [...] was still the cause of more significant concern among informants due to its wide-ranging reporting obligations stretching across the entire supply chain."

Nordic MNCs have developed pragmatic coping mechanisms, such as:

- heavy investment in compliance programmes and experienced in-country teams to navigate nebulous and rapidly changing compliance demands;
- restructuring and local adaptation of operations, which include "China-for-China" models for data, IT systems and supply chains;
- selective use of legal and operational workarounds to avoid direct conflicts (e.g. commercially framed decisions instead of explicit references to sanctions);
- informal engagement with local authorities in the PRC to maintain operational continuity; and
- limited but targeted policy engagement through business networks.

Implementation of coping mechanisms relies on risk-based judgment by senior officers, and requires pragmatism and adaptability to a changing landscape. This means that companies face difficult decisions that are frequently made in-country, sometimes with limited headquarters oversight, but potentially with global risk management impact. Thus, the strength of relationships and communication channels between in-country staff and HQ are instrumental. Global risk oversight increasingly relies on tailored local implementation in a PRC context, which increases vulnerability to geopolitical tensions between countries.

Despite the extensive requirements imposed by legislation, Nordic MNCs often take on even more stringent operating standards through their own codes of conduct. This adds an additional layer of complexity to questions of labour rights, advocacy work and supply chain or customer scrutiny, but can at the same time be an asset when designing compliance dilemma coping mechanisms. Companies may increasingly point to a code of conduct as the gold standard to which they hold their behaviour.

"Local workers insisted on working as many hours as possible during peak season. There was a real risk of losing staff to competitors with less stringent Code of Conduct practices if they were not allowed to do so."

Respondent discussing the impact of Code of Conduct dilemmas.

Compliance work in the PRC should be perceived as a “craft” that requires judgment, relationships and experience, in addition to knowledge of formal rules. Honing this craft could become a competitive edge for Nordic MNCs as geopolitics and supply chain challenges increasingly become normal parts of international business. However, this will require a sober assessment of an extraordinarily complex compliance landscape combined with continued investment in research and training. Nordic MNCs could benefit from their traditionally close and constructive relationships with Home Country governments and academia to make further progress in this regard.

In order to support Nordic industry as it adapts to the compliance dilemmas encountered in the PRC, and to reinforce the coping mechanisms adopted by individual Nordic MNCs in their PRC operations, this study **recommends that stakeholders:**

- **Adjust Nordic MNC corporate risk models as supply chains are increasingly viewed through a national and economic security lens in the PRC, Europe and beyond.** A risk-based approach that assumes lax enforcement by PRC government agencies appears increasingly unsustainable.
- **Develop a better understanding of hidden compliance risks in relationships between Nordic MNC HQs and in-country operations**, for example in relation to global enterprise management software and the siloing of data.
- **Renew and intensify dialogue between government and business** to unpack the multifaceted challenges of geopolitically impacted corporate compliance. Consider ways to measure returns on investments made in compliance programmes.
- As China-for-China strategies are now being introduced, in part due to the increasing burden of externally imposed compliance dilemmas, **consider how future regulation could to a greater extent rely on progressive initiatives in areas such as labour rights and environmental protection** that are already under way through the codes of conduct of many Nordic MNCs..
- **Map shortcomings in the compliance capabilities of SMEs to avoid disproportionate accumulation of risk** among those businesses least able to cope with the growing compliance burden.

1. Introduction

a. Objectives

This study seeks answers to a series of research questions regarding (i) whether Nordic multinational companies (MNCs) encounter compliance dilemmas in connection with their operations in the PRC; (ii) the impact compliance dilemmas have on operations; and (iii) how MNCs manage the resulting risks.

The topic is currently little discussed, let alone understood, so the findings will serve to enhance the collective knowledge base among the business community. Given an international environment characterised by a growing body of extraterritorial legislation on national security, data security and corporate sustainability, the risks posed by compliance dilemmas are set to increase for the foreseeable future.

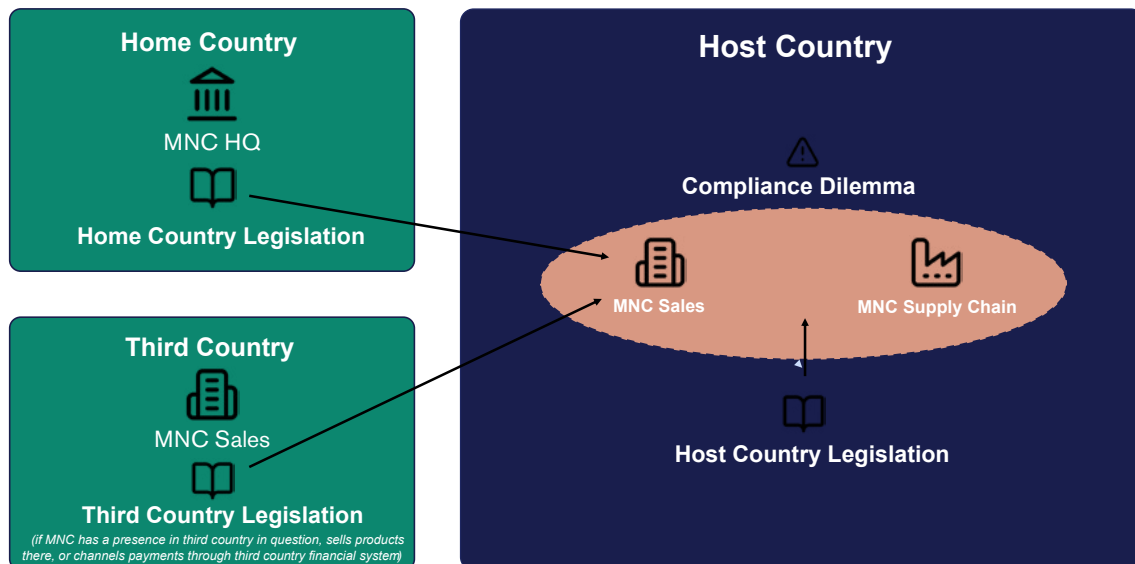
An understanding of compliance dilemmas would leave individual companies better equipped as they go about formulating their PRC strategies. The findings may also form part of future government policy considerations, for example when it comes to the impact of compliance dilemmas on the operations and strategy of MNCs.

b. Compliance Dilemmas

i. What are Compliance Dilemmas?

Traditionally, businesses have only had to pay attention to the laws of one country at a time. The national legislation of Finland or Sweden (including EU law), for example, did not apply to a Nordic MNC's operations in the PRC. Similarly, PRC legislation would traditionally have had little or no bearing on the activities of a Nordic MNC outside the PRC. Today, the situation has become more complicated as jurisdictions increasingly work to increase their extraterritorial reach. This section reviews the main Home Country, Host Country and Third Country legislation that could give rise to compliance dilemmas. A tabular summary of the relevant laws is found in Appendix A.

Home Country	Jurisdiction where the MNC headquarters is located. For the study participants, this is Finland or Sweden. Both these countries are EU member states, so EU law is by default considered Home Country legislation.
Host Country	Jurisdiction where the MNC supply chain is located and where the MNC often also has significant sales activities. Unless otherwise stated, the term Host Country when used in the study refers to the PRC.
Third Country	Jurisdiction with extraterritorial features that impact MNC Host Country activities.



Home and **Third Country** legislation reaches into **Host Country** operations, where it may conflict with **Host Country legislation** governing all local MNC activity.

- Home Country legislation imposes requirements on MNC behaviour in the Host Country, for example with regard to EU supply chain rules.
- Third Country legislation can impose a separate set of requirements on an MNC's activities in the Host Country, depending on whether or to what extent the MNC has a presence in the Third Country or wishes to sell its products there.
- Host Country legislation governs all of the MNC's activities in the Host Country and may come into conflict with activities undertaken as a result of Home Country or Third Country legislation.

The term “compliance dilemmas” has emerged in researchⁱ to describe some of the situations that are the focus of this study. Published research has dealt specifically with the legal tensions and corporate compliance issues that result from political tensions between the United States and the PRC. In this study, however, the term is used more broadly in relation to the compliance challenges faced by MNCs in the PRC.

ii. The Home Country Dimension

This study was initiated with an awareness that Nordic Home Country legislation has recently introduced new demands on Nordic MNC overseas supply chain reporting and due diligence practices. This has mainly taken the form of a series of EU legislative measures, notably the EU Corporate Sustainability Reporting Directive (CSRD) which covers not only environmental reporting, but also social aspects such as human rights, as well as governance aspects like the absence of corruption.¹

The EU Corporate Sustainability Due Diligence Directive (CSDDD) requires companies that do business in the EU to conduct due diligence to identify, prevent, mitigate and remedy human rights and environmental harms in their own operations and in the operations of

1

A category of “Environment Social and Governance” reporting often abbreviated as ESG.

their subsidiaries and business partners across the globe. Companies that fail to fulfil their CSDDD obligations risk substantial fines of up to 3 percent of worldwide turnover.

The CSRD and the CSDDD, enacted in 2022 and 2024, respectively, have recently been the subject of drawn-out review and amendment processes, including so-called Omnibus amendments agreed in 2025 and early 2026.²

While the CSRD and the CSDDD, along with other EU legislation such as the Carbon Border Adjustment Mechanism, the Deforestation Regulation and the Forced Labour Regulation (each of which is at a different stage of implementation) were the main focus of this study, several other pieces of national and EU legislation could come into play for Nordic MNCs in the PRC. For example, Home Country data legislation, such as the EU General Data Protection Regulation, was raised at times during the study, as were Home Country anti-corruption laws.

iii. Export Controls and Sanctions

Nordic MNCs are subject to export controls targeted at physical goods, software, technology, data and services that are designed for military end-use, or which have “dual-use applications” (civilian and military). Such export controls exist in relation to Nordic Home Country components and software intended for export to the PRC and in relation to any Third Country (including US) content incorporated into Nordic Home Country exports. In the case of the PRC, the United States has introduced export restrictions with respect to advanced artificial intelligence (AI) chips and graphics processing units (GPUs), certain semiconductor manufacturing equipment and some chip design software.

International trade has gone through a process of politicisation, as evidenced by the now extensive network of sanctions introduced by different countries against organisations and individuals that, one way or another, are deemed threats to national interests. In particular, the United States maintains Entity Lists that ban transactions with listed PRC individuals and organisations.

Export Control Measures (“WHAT” an MNC trades)	Sanctions (“WITH WHOM” an MNC trades)
Regulate the transfer of specific items (goods, software, technology, services)	Restrict or prohibit dealings with certain countries, entities, sectors or individuals
Focus on national security and sensitive technology	Focus on broader foreign policy, security, human rights or geopolitical goals
Rely on - control lists (classified items) - licensing requirements - end-use and end-user screening	Rely on - blocked persons lists - countrywide embargoes - sectoral prohibitions - asset freezes
Typically cover - advanced semiconductors - encryption software - military components - dual-use equipment	Typically cover (in relation to listed entity) - sales to - receiving payment from - providing services to - engaging in financing with - maintaining contracts with

² Omnibus narrowed the original scope of the CSRD and the CSDDD so that mainly larger companies are targeted. Requirements have also been eased. For example, there will now be less of a requirement to perform due diligence beyond first tier suppliers under the CSDDD. (The obligation to perform due diligence further down the supply chain is only triggered on receipt of plausible information of harm.) Implementation of the directive has also been postponed.

Sanctions regimes typically apply to the sanctioning country's own citizens and companies (so-called primary sanctions). Increasingly, however, sanctions are also used to exert leverage over foreign individuals and companies (secondary sanctions). From the viewpoint of Nordic MNCs, US secondary sanctions are of particular concern. These are sanctions whereby they as "Third Country organisations" may be penalised by the US government for trading with PRC counterparts that, in turn, are deemed to have engaged in sanctioned business activities with, for instance, Russia or Iran.

Primary Sanctions	Secondary Sanctions
Apply to - citizens and permanent residents of the sanctioning country - companies incorporated in the sanctioning country	Apply to - non-nationals - non-resident foreign companies - transactions occurring entirely outside sanctioning country
If triggered - civil or criminal penalties - asset freezes - imprisonment - loss of export privileges	If triggered - loss of access to sanctioning country's financial system - prohibition on US dollar clearing (in US context) - blocking sanctions imposed on foreign firm (property frozen, sanctioning country parties banned from dealing with sanctioned party)

Distinct from export controls and sanctions, but still relevant to the study, are third country laws and regulations that impose non-tariff barriers in relation to imports from the PRC. Of particular interest to Nordic MNCs is the US Uyghur Forced Labor Prevention Act, which severely restricts the scope for US imports originating from, or related to, the PRC's Xinjiang Uyghur Autonomous Region.

iv. The Host Country Dimension

The PRC has recently introduced new national security, cybersecurity and personal data laws. In some cases, these laws should be understood in the context of a more polarised international security climate. For example, PRC laws on State Secrets, Counterespionage and Foreign Relations aim to protect core national interests, in part by relying on vague terminology for concepts such as "national security" and "state secrets".

There is a clear trend in PRC legislation and policy, further emphasised by two March 2026 State Council decrees, for supply chain security to be considered a national security concern. The PRC government wants to be ready to deal with "improper" foreign intervention in its supply chains, for example, through legislation with extraterritorial application.³

³ State Council decree no. 834 (Provisions of the State Council on the Security of Industrial and Supply Chains) and no. 835 (Regulation of the PRC on Countering Foreign States' Improper / Unlawful Extraterritorial Jurisdiction), see also Appendix A.

This could mean that the lack of clear definition of “state secrets” and “important data” (see below in relation to Data Security Law) takes on an even greater urgency in the compliance departments of Nordic MNCs.ⁱⁱ

Governments around the world have introduced legislation intended to provide tools that will help to protect core national interests in the context of international trade. For the PRC, this toolkit comprises legislative measures such as the Unreliable Entity List, PRC Blocking Rules and the Anti-Foreign

Sanctions Law, all of which, at least in part, were enacted for the purpose of preventing, or limiting the impact of, foreign trade measures deemed by the PRC to be targeting its interests in an unfair manner. For example, the PRC Blocking Rules provide a broad legal framework for countering the impact of foreign laws with extraterritorial application on the PRC.

Another development that is not unique to the PRC, but which nonetheless has consequences for business, is the increasing body of legislation around data security. This is manifest, among other things, in the PRC Cybersecurity Law of 2017, the Data Security Law of 2021 and the Personal Information Protection Law, also of 2021.

v. Codes of Conduct

In addition to binding legislation, whether enacted by the Home Country, the Host Country or a Third Country, the activities of MNCs are guided by internal working documents, which are referred to in this study as Codes of Conduct. Such codes typically detail an MNC's practices and procedures in key areas of its operations, such as production, sourcing and data management. While the specific content of a Code of Conduct is ultimately determined by the MNC itself, as a result of the CSDDD,⁴ the decision to adopt a code in the first place may no longer be discretionary for Nordic MNCs.

Naturally, MNCs design their Codes of Conduct in order to meet relevant legal requirements. However, they typically go beyond the letter of the law to provide an operational standard that is deemed to be in line with the MNC's corporate culture, which might be influenced by a diverse range of considerations, not least customer expectations and the risk of adverse media reporting.

Various reporting has shown how an MNC's Code of Conduct may give rise to compliance dilemmas; for example, when international fashion brands faced a backlash in the PRC having declared that they would cease to buy cotton produced in Xinjiang.ⁱⁱⁱ

Since MNCs tend to refer to their Codes of Conduct when explaining their actions, this study has treated its Participants' Codes of Conduct as a source of norms distinct from legal requirements imposed by Home Country, Host Country or Third Country governments, as the case may be.

”There is a clear trend in PRC legislation and policy, further emphasised by two March 2026 State Council decrees, for supply chain security to be considered a national security concern. The PRC government wants to be ready to deal with “improper” foreign intervention in its supply chains, for example, through legislation with extraterritorial application.”

⁴ Article 7 of the CSDDD mandates that as part of their due diligence obligations, in scope companies shall maintain a Code of Conduct “describing rules and principles to be followed throughout the company and its subsidiaries, and the company's direct or indirect business partners”, and that the company's due diligence policy shall describe “the measures taken to verify compliance with the code of conduct”.

"Naturally, MNCs design their Codes of Conduct in order to meet relevant legal requirements. However, they typically go beyond the letter of the law to provide an operational standard that is deemed to be in line with the MNC's corporate culture, which might be influenced by a diverse range of considerations, not least customer expectations and the risk of adverse media reporting."

vi. How Compliance Dilemmas arise

Nordic MNCs implementing the CSRD, the CSDDD and other EU supply chain rules find themselves asking their suppliers a lot of questions about environmental matters, social aspects and governance issues. EU rules make clear that merely asking questions and collecting supplier statements is not sufficient. Instead, companies that fall within the scope of the CSRD need to have put in place controls, including formal policies approved by management, as well as clear procedures on oversight and assignment. As with financial reporting, these controls need to be available for inspection by auditors. Similarly, the CSDDD requires MNCs to implement extensive policies and procedures designed to systematically minimise undesirable supply chain practices.

This all boils down to an expectation that MNCs will be active in the field, including follow-up investigations and site visits wherever circumstances suggest these may be needed. As mentioned above, a Nordic MNC selling PRC-manufactured goods into the US market must also comply with US law, including the US Uyghur Forced Labor Prevention Act (UFLPA). Here, the evidentiary burden is even higher as companies must overcome a "rebuttable presumption" that forced labour has been involved in the supply chain. Inquiries into UFLPA matters would typically be considered highly sensitive in the PRC. In fact, a high-profile US fashion company was placed under investigation by the PRC's Ministry of Commerce in 2024 for allegedly taking "discriminatory measures" against products from Xinjiang.^{iv}

"Thus, as Nordic MNCs engage in Q&A exercises with suppliers and deploy their staff to sites far and wide across the PRC, questions may arise about the boundaries placed by PRC law on the scope of such due diligence activities. Similarly, even where data can be legally collected, it is open to question whether Nordic MNCs are able to store and process it in accordance with PRC law."

Thus, as Nordic MNCs engage in Q&A exercises with suppliers and deploy their staff to sites far and wide across the PRC, questions may arise about the boundaries placed by PRC law on the scope of such due diligence activities. Similarly, even where data can be legally collected, it is open to question whether Nordic MNCs are able to store and process it in accordance with PRC law.

Since compliance functions are almost always managed at group level, it will be critical to ascertain whether due diligence data can be legally exported out of the PRC. A compliance dilemma would arise if PRC law raises questions about or obstacles to the due diligence activities required by Nordic MNCs under EU supply chain rules.

Even more clear-cut compliance dilemmas arise whenever a Nordic MNC refrains from doing business with a PRC counterpart due to international sanctions or export control rules. Here, PRC Blocking Rules may come into play, potentially placing the Nordic MNC in what is a pure compliance dilemma. The Nordic MNC's actions would breach Home Country (or Third

Country) legislation if the contemplated transaction went ahead, whereas PRC Blocking Rules make clear the potential for Host Country legal consequences (both civil and criminal) if the transaction does not go ahead.

c. Methodology

i. Participants

The study's original data is from qualitative interviews with senior personnel at six MNCs headquartered in Sweden or Finland. These were large publicly listed MNCs with global operations as well as smaller MNCs with a more limited geographic footprint. Potential participating MNCs were approached through the professional networks of the project team members. Individual Informants were then designated from within the organisations that agreed to participate in the study.

Between one and three individuals Informants were interviewed from each Participant. When a Participant had more than one Informant, either multiple interviews were carried out with Informants separately or several Informants joined a single session. Informants collectively provided insights into how Participants' PRC compliance operations were structured, and findings in this regard are included in Appendix B.

One SME Participant provided a contrasting perspective. Unlike larger firms, this company operated without dedicated legal or compliance staff, relying instead on ad hoc internal coordination. As the Informant noted, compliance work is *"like an ad hoc thing...we act when we need to"*.

While the number of participating companies was relatively small, they did, as noted above, include companies of different sizes. In addition, they spanned a broad range of industries and represented different types of ownership (private and public), as well as different organisational structures (highly centralised or decentralised).

ii. Interviews

The study used semi-structured interviews as its primary data collection method. Each interview started with a set of questions, which was followed by follow-up questions; the questions were the same for all respondents but greater emphasis could be placed on certain questions during the interviews, depending on how the interview unfolded and which themes became dominant. Thus, while the interviews followed the same structure, the emphasis placed on individual questions could vary. This type of interview provides a structural framework of questions but, at the same time, allows the Informants to elaborate on their thoughts and answers. It also enables the interviewer to adapt and adjust the order of the questions. It provides a structured but adaptable format, enabling unanticipated insights to emerge during the interview process. An interview guide with questions sent to the Informants in advance helped to formulate and structure the questions. The Participants were approached for interviewees through partners, such as chambers of commerce.

iii. Implementation

The interviews were conducted between October 2025 and April 2026 with Informants who worked as in-house lawyers, procurement managers, compliance officers or business unit managers. The interviews were conducted individually via a digital platform. Each interview

lasted for between 60 and 90 minutes. Prior to the interviews, Informants were informed of the objectives of the study, the questionnaire, the interview process and their rights, including the right to withdraw at any time without consequence. With informed consent, all the interviews were audio recorded and subsequently transcribed to ensure accuracy and enable systematic analysis. The transcription was carried out using an AI tool. The interview transcripts were checked manually by members of the research team. Recordings and transcripts were permanently deleted on completion of the study.

iv. Materials

This study draws on various types of data to shed light on the issues surrounding compliance for Nordic MNCs in their operations in connection with the PRC. The main material comprises semi-structured interviews conducted with representatives of Swedish and Finnish multinational companies. In addition, data from several business confidence surveys conducted by international chambers of commerce has been included to provide contextual background and an overview of compliance issues.

Drawing on existing surveys enabled the study to identify analytical gaps (e.g., regarding the concerns companies have in relation to the ambiguous regulatory environment) for the qualitative interviews to address in greater depth. The surveys also served as a contextual foundation for the development of the interview guide, ensuring that the questions reflected empirically grounded issues of significance to the industry.

d. Background: Business Sentiment and Compliance Challenges

This section draws on recent business confidence surveys conducted by the European Union Chamber of Commerce in the PRC, the American Chamber of Commerce in the PRC and Nordic chambers of commerce to outline how MNCs perceive the business climate in the PRC.^v The EU and US surveys are perceived as leading barometers of international business in the PRC.

Across the surveys, the overall picture is one of a more cautious and, in many cases, deteriorating business outlook, consistent with general media reporting on the topic of the PRC's foreign investment environment.^{vi} Among European firms, a substantial majority reported that operating conditions have become more difficult, while confidence in short-term growth is limited. This shift reflects not only macroeconomic pressures, but also a regulatory environment that has become more complex, politicised and difficult to navigate. At the same time, Nordic companies stand out as comparatively more resilient, with a larger share continuing to express medium-term optimism and willingness to invest.

A set of persistent structural challenges emerged consistently across the surveys. Chief among these are an ambiguous legislative environment, regulatory unpredictability and an increasingly pronounced disconnect between headquarters expectations and in-country realities. Companies also highlight the growing importance – and difficulty – of managing compliance in areas such as data security, cross-border data flows and supply chain transparency.

The survey results further suggest that while compliance challenges are widely recognised, their nature and severity vary significantly across sectors and risk areas, underscoring the need to move beyond aggregate indicators to understand the operational dynamics facing individual firms.

i. A challenging business climate overall

Recent surveys highlight a marked shift towards greater uncertainty and caution in business sentiment. Many firms are adjusting their expectations, with greater emphasis on cost control and risk management rather than expansion.

Among US firms, the picture is more mixed. While some report stable or improving profitability, there is continued sensitivity to geopolitical dynamics, particularly the bilateral relationship between the PRC and the United States. A large majority emphasise the importance of this relationship for their future prospects, even as concerns persist regarding inconsistent regulatory interpretation and enforcement.

Despite these pressures, Nordic firms exhibit a relatively more balanced outlook, and many continue to plan for growth and investment in the PRC.⁵ This suggests that while the operating environment has become more demanding, the PRC remains strategically important – especially for companies with established market positions or long-term commitments.

ii. China -for-China and supply chain adjustments

There is a pronounced trend for a gradual “siloeing” of PRC operations, as companies seek to manage geopolitical risk and regulatory divergence. Firms are increasingly seeking to separate PRC-focused activities from global systems for supply chains and data infrastructure, as well as organisational structures.⁶

This has contributed to a wider bifurcation of global supply chains, which is often described as derisking or China-for-China. Firms are localising certain activities within the PRC while at the same time diversifying production elsewhere.

A majority of US firms (71 percent) are not actively relocating production. However, the still not trivial minority that are relocating cite geopolitical tensions (40 percent) and risk management considerations (36 percent).⁷

iii. Regulatory landscape: ambiguity and unpredictability

Chambers of commerce are unequivocal that the lack of a clear definition of concepts such as “national security” in PRC legislation, considered in the context of the far-reaching due diligence obligations set out in Home Country legislation, such as the EU supply chain rules, create serious compliance challenges for MNCs in the PRC.^{vii}

A central theme in all the surveys is the lack of clarity and predictability in the regulatory environment in the PRC. European companies frequently cite ambiguous rules and inconsistent enforcement as major obstacles to both day-to-day operations and longer-term planning.

5 31 percent of Swedish companies planned to increase investment in China in 2025.

6 For example, the European Union chamber of Commerce survey found that 63 percent of participants were reviewing their supply chain strategies: 32 percent were “onshoring” into the PRC while 7 percent were “offshoring” away from the PRC; 24 percent of participants were both “onshoring” and “offshoring” at the same time.

7 For example, among Swedish companies, only 9 percent had not at least reviewed their supply chain strategy. A majority (54 percent) of Swedish companies had concluded that they would either not make any changes to their supply chain strategy or increase their PRC footprint. A relatively small minority (11 percent) had plans to diversify supply chain away from China (offshoring).

This uncertainty is compounded by the interaction between Host Country regulation and the extraterritorial requirements of Home and Third Countries, particularly in areas such as sustainability reporting, export controls and sanctions compliance.

"A substantial number of firms expect EU directives such as the CSDDD to materially impact their PRC operations. This illustrates the growing entanglement of regulatory regimes despite the fact that the Omnibus reforms were intended to ease the compliance burden."

A substantial number of firms expect EU directives such as the CSDDD⁸ to materially impact their PRC operations. This illustrates the growing entanglement of regulatory regimes despite the fact that the Omnibus reforms were intended to ease the compliance burden .

Incidentally, various organisations voiced concerns about the overall level of understanding of the CSDDD and related legislation in the business community.^{viii}

External regulatory developments – especially from the United States – are also seen as having had spillover effects for PRC operations, adding to compliance costs and operational complexity. A more transparent and predictable regulatory environment is widely seen as a key requirement for restoring investment confidence in the PRC.

In the area of data governance, companies acknowledge incremental improvements in regulatory clarity, particularly regarding cross-border data transfers. However, overall satisfaction remains low and uncertainty persists around key definitions and practical implementation.

2. Findings

a. Four Types of Compliance Dilemma

Four categories of compliance dilemma were identified in the Informant interviews.

Pure compliance dilemmas	Home Country legislation or Third Country legislation clearly mandates Action X but Host Country legislation clearly prohibits Action X, meaning that the Participant risks being in breach of binding legislation regardless of whether Action X is taken.
Home Country-driven compliance dilemmas	Home Country legislation mandates Action X. At the same time, Host Country legislation or the policy environment either makes Action X practically difficult to implement or makes the consequences of taking Action X difficult to foresee.

8 The European Union Chamber of Commerce survey found that 45 percent of participants expected to be impacted by the CSDDD. (No separate measure was reported for firms expecting to be impacted by the CSRD.)

Host Country-driven compliance dilemmas	Host Country legislation prohibits Action X. Action X is not mandated by the Home Country or Third Party, but it is the desired course of action for the Participant. Host Country legislation therefore creates a dilemma.
Code of Conduct-driven compliance dilemmas	Implementing a Code of Conduct presents challenges as a result of the Participant's Code of Conduct being stricter than applicable legislation.

These four types of dilemma are intended to facilitate the reader's grasp of the PRC compliance challenges faced by Participants. They are not necessarily the final word on how to categorise the issues discussed. It should be noted that a single action could fall into several categories.⁹

b. Pure Compliance Dilemmas

i. Triggered by sanctions and blocking legislation

Informants described scenarios where Home Country or Third Country legislation mandated certain actions, which, if taken, would invoke PRC Blocking Rules. The most common such scenario is straightforward compliance with Home Country or Third Country secondary sanctions, according to which sales of products containing certain technology or components to sanctioned PRC entities are banned. PRC Blocking Rules threaten the application of PRC sanctions to a party that refrains from selling to PRC entities due to foreign sanctions. A Participant in this situation therefore has cause for concern.

Participants were generally aware of the potential impact of sanctions on their operations but appeared relatively comfortable with their ability to manage this type of compliance dilemma. One Informant stated that, while they were aware of the PRC Blocking Rules and their global scope, they believed the PRC's ability to monitor international compliance was limited.

"Neither the PRC nor the EU has been great on extraterritoriality. I think the US has always been great, whether we speak about sanctions, regulations and enforcement, or anti-bribery and corruption legislation and enforcement."

Participant compliance director putting the threat of PRC extraterritorial sanctions into perspective.

None of the Informants reported issues arising from military end-user sanctions, mainly because the Participants' products are generally not dual use. Some Informants reported that their companies supply military organisations, but the products involved were deemed low risk.

⁹ For example, Code of Conduct-driven compliance dilemmas might fit into either a Home Country- or a Host Country-driven compliance dilemma, depending on the source of a given Code of Conduct norm. Since Informants often focused on their Code of Conduct rather than any underlying legislation, Code of Conduct-driven compliance dilemma was retained as its own analytical category.

ii. Work institutionalised

Several Participants highlighted sanctions monitoring as an area of compliance where companies have successfully institutionalised their work, meaning they are able to rely on clear organisational work processes supported by broadly available technology. Sanctions management work has been an increasing trend in corporate life for many years and a collective knowledge base seems to have taken shape, at least among the larger companies. The sanctions regimes (whether Home Country, Third Country or Host Country) are transparent and the Participants reported wide access to monitoring software, which provides compliance officers with powerful tools to support their work. At least in theory, this puts companies in a good position to avoid pure compliance dilemmas.

iii. The risks are real

In practice, however, pure compliance dilemmas still arise. One Participant had had to cancel sales on multiple occasions after discovering that its counterpart was sanctioned. While the Participant aims to detect sanctioned companies before agreements are concluded, these checks can fail. Moreover, since the Participant has a policy of openness vis-à-vis its customers when an order is cancelled, it provided the customer with full disclosure of the reasons behind the decision. (Other Participants chose to invent a commercial pretext.) The Participant was not overly concerned about exposure to the PRC Blocking Rules, noting that the sanctioned counterpart also had an interest in keeping a low profile about the matter.

Nonetheless, there are real concerns about Pure Compliance Dilemmas and this is an area where large companies with complex global footprints at times face delicate questions.

"At the end of the day, we are kind of falling in between. We are an EU registered corporate that has a significant presence in the US, and equally significant in the PRC as well. So it comes back to how you balance [compliance obligations]. Looking at it from a sanctions perspective, do we need to comply with primary US sanctions? Do we need to be concerned about US secondary sanctions? It's always a risk-based approach and you can't really get a one-size fits all [solution] to fit the whole umbrella. So you need to chop it up a little bit."

Participating compliance director regarding the complexity of the environment they are trying to navigate.

iv. Workarounds

While recognising the legal significance of Home Country and Third Country sanctions, Participants viewed related problematic areas through a pragmatic lens and were prepared to consider workarounds that they felt could be deployed without legal risk. These workarounds might be designed to eliminate risk by avoiding individual transactions or entire customer relationships. Alternatively, supply chains could be remade, removing any sanctions exposure that might have previously existed.

One Informant spoke of their company's routine sanctions checks and saw the risk of repercussions from discovering a sanctioned counterpart as low. According to the Informant, the company aimed to minimise risk by declining a transaction due to sanctions but referring to commercial reasons that would be acceptable to the counterpart, thereby handling the case "behind the scenes".

On finding an equipment supplier to be the target of sanctions, another Participant launched a new bidding round with modified criteria designed to exclude the sanctioned supplier. In this way, the Participant was able to avoid a situation where it might have to admit to a PRC authority that a supplier had been rejected due to foreign sanctions.

Some workarounds are potentially more costly than others. One Participant decided to discontinue an entire product line produced in Europe in order to avoid the risks associated with sales to Xinjiang. The product in question had a significant customer located in that region. Rather than risk the legal or media exposure in the PRC that might result from rejecting sales on a targeted basis, the product was simply removed from the Participant's offer.

One Informant noted bluntly that there are "always workarounds" when dealing with sanctions. They reported the possibility of reworking supply chains to exclude the sanctioning country, typically in a "PRC-only" solution.

"If you see the business needs, then you work around the sanctions. There are always ways to get round the sanctions, for example with our China-for-China policy. If you make a PRC product without US technology, you can still be compliant and not violate any sanctions laws."

Participant compliance director on the availability of sanctions workarounds.

c. Home Country-driven Compliance Dilemmas

Within this category, most of the discussions with Informants revolved around the CSRD, the CSDDD and related EU supply chain legislation. Informants raised the administrative burden involved in compliance with the CSRD, as well as concerns over the future impact of CSDDD compliance, which could require extensive oversight obligations with regard to complex supply chains.

Several Participants were either already implementing the CSRD or in the process of developing implementation procedures. While Informants were concerned about increasing compliance workloads, by and large they gave the impression that CSRD implementation has been orderly and manageable. One Informant explained how their long-standing supplier relationships were of great value when, like now, there is a need to implement new reporting standards.

One Informant described their company's CSRD compliance process, highlighting how the filing requirements involve several thousand items of data. With two company employees responsible for this reporting project, they described the cost as "not insignificant" while – as they saw it – generating limited value. However, a Participant that had completed CSRD implementation, reported that the workload was not particularly high. It is likely that this divergence in experiences could, at least to some degree, be explained by different levels of supply chain complexity among Participants.

By contrast, the CSDDD, which is yet to be implemented and has had its impact softened by the EU Omnibus legislation, was the cause of more significant concern among Informants due to its wide-ranging reporting obligations that stretch across the entire supply chain, particularly in its pre-Omnibus form.

Participants' concerns were rooted in the immensity of the task of cataloguing vast supply chains. Some Participants have thousands of suppliers in the PRC when second and third tiers are included. In addition, there was an awareness, built on the voluntary Code of Conduct-based due diligence reporting carried out by many Participants for several years, of the challenges involved in obtaining reliable data from suppliers. Some Participants highlighted that the PRC poses particular challenges in this regard as there are, in their experience, well-documented problems when it comes to being able to access objectively verifiable counterpart information. At times, Participants would have to consider whether counterpart self-certification could meet the due diligence threshold.

"In discussions with PRC counterparties, what sometimes happens is that the counterparty takes the position that, yes, we can sign the assurance that you need. Can you please provide us with the document? This is, of course, not an approach that would provide us with the needed assurances. It's a paper trail only."

Participant legal counsel regarding the limited options for overcoming a lack of transparency in PRC counterpart vetting.

The inherent unreliability of this type of self-certification was, in a sense, underlined by the one SME that participated in the study. While it had a high level of trust in its own supply chain, based on years of working with a core group of suppliers, it lacked the means to verify key supplier information independently. Despite this serious limitation, the SME's Informant said that they would in the end sign off on customer due diligence forms themselves while "crossing my fingers".

"When it comes to our responsibility for not just [our first-tier supplier] but [supplier's] subcontractors, and even the subcontractor's subcontractor, and so on... we have put a large question mark on whether this could be done in a sensible way. [...] And it's not because it's the PRC, it's because it's just not possible."

Participant CEO with concerns about potential future CSDDD implementation.

Other Participants emphasised that while the PRC might present its own challenges in some areas, their concerns with respect to sustainability reporting and due diligence were for the most part not unique to the PRC.

Rather than conduct comprehensive due diligence checks on each individual supplier, several Participants reported taking "risk-based" approaches in which direct vetting efforts would typically focus on first tier suppliers. Within such a risk-based approach, the Participant would then – as allowed for by the CSDDD – employ a combination of supplier self-certification and proprietary risk evaluation frameworks to evaluate its broader network of suppliers.

In addition, Participants that use a risk-based approach group suppliers based on their strategic importance to the supply chain. If there are few alternative suppliers of a certain component, this could lead to the small second tier supplier from which that component was sourced being classed as strategically important and therefore requiring in-depth vetting. Another parameter taken into account as part of risk-based frameworks is the degree to which any links in the supply chain might be exposed to high-risk sectors such as the defence industry.

Participants that deal with wood products pointed out that the EU Deforestation Regulation, like the (pre-Omnibus) CSDDD, contains multi-tiered supply chain due diligence obligations, which is a source of some concern.

d. Host Country-driven Compliance Dilemmas: PRC data legislation

The most common situations in which Host Country legislation was the main trigger of compliance dilemmas concerned the PRC's evolving data legislation. This section examines Participants' experience of compliance dilemmas emanating from: (i) the collection, use and storage of important data and "national core data" in their operations; (ii) personal data, including that of employees and customers; and (iii) conflicts between the letter of the law, on the one hand, and application of the law, on the other.

i. Handling sensitive data

PRC data legislation relies on terms such as "important data" and "national core data", which are vaguely defined. In certain situations, such as when national core data is involved, data must be stored onshore. Participants reported various degrees of exposure to important data as defined in PRC law. Some Informants described complex situations around data compliance. However, even Participants in similar sectors often had diverging experiences – possibly as a reflection of different compliance practices inside Participants.

Important data, which is defined in the Data Security Law as "data that, if tampered with, destroyed, leaked, illegally obtained or used, may endanger national security, economic operation, social stability, public health and safety", is a key term throughout the PRC's legislation that helps to determine the level of safeguards needed in data processing and storage. In some cases, it also prevents the export of data.

Important Data is defined as "data that, if tampered with, destroyed, leaked, illegally obtained or used, may endanger national security, economic operation, social stability, public health and safety
PRC Data Security Law.

Some Participants offer connected products or other "internet-of-things" services that are based on data collected during operations. One Participant reported that such individual data cannot be transferred out of the PRC for customized processing, for instance in connection with customer support, at an overseas location, although it could be transferred for analytical purposes without identifying features. This means that customer-facing data functions had to be performed in-country. Participants did not report any negative fallout from this adaptation to PRC data requirements.

Participants mentioned other types of sensitive data during operations. A notable category is geographic data, which may include location information on sites considered sensitive in the PRC, such as military installations. However, while one Informant considered the potential risk to be significant, compliance was also deemed to be relatively straightforward, and such data was not transferred abroad.

"It was clear that this is considered a national secret and should not be cross-border transferred outside of the PRC. We had to do a lot [of work] to comply. [...] So, for example, the PRC team from time to time would have exchanges with the European experts, and during those communications someone might just send over [a file containing national secrets]. So it's almost impossible to control other than just to [implement] training and make sure that people understand, and then it's only authorised persons who have access to this sensitive data."

Participant in-house lawyer on how to implement compliance framework regarding sensitive data.

Sometimes, product development in industry areas is treated by the PRC's national strategic focus areas^{ix} as sensitive for cross-border collaboration; for example, where a Participant has research and development staff in both the Home Country and the PRC. Informants reported relying on a combination of internal compliance frameworks to regulate data transfer and use and structural arrangements with their PRC suppliers to mitigate risk. However, they also emphasised that the mutual trust that results from long-standing partnerships was important in mitigating doubt.

"We have a liaison office in [the Nordics] that is actually owned by [the supplier]. So there are ways obviously to transfer documentation. I know that it is sometimes problematic but we are definitely coping with it."

Participant compliance director discussing data transfer policies.

ii. Personal data dilemmas

For Participants with limited exposure to important data, personal data processing was often the biggest concern with data compliance. While some Participants stated that cross-border data transfers were limited to human resources and systems for managing customer and supplier relationships, other Participants depended on global integration of a wider range of operational systems. Overall, globally integrated IT functions were a common theme among Participants and compliance with personal data management was a concern for all Participants, regardless of size and industry.

Informants frequently discussed their companies' use of globally integrated human resources or customer relationship management (CRM) systems, often via external providers. In these cases, storing data in the PRC alone would create significant hurdles for global operations. In addition, some external providers were unable to provide "PRC-only" storage. While the Personal Information Protection Law has certain exceptions for data transfer, many Informants reported following "best possible" practices. These included following the rules of the EU General Data Protection Regulation, which were seen as providing a degree of credibility even though they have no legal validity in the PRC, while also seeking PRC legal advice to prepare for or avoid potential risk scenarios.

"We actually did this kind of due diligence with external law firms to study all the systems regarding cybersecurity and data processing. And then [the law firm] provided a map of which [practices] are in violation of PRC law and regulations, and what kind of solution you need to implement."

Participant in-house lawyer discussing data risk assessment.

Participants reported collecting personal data not only for group-wide systems, but also to comply with internal risk management policies. One Informant explained how they were using an in-house tool to track conflicts of interest among employees with regard to supplier companies. The tool mapped potential family relationships between the Participant and suppliers, and therefore required extensive personal data inputs in relation not only to employees, but also to their family members and even the family members of suppliers. According to the Informant, submitting data was mandatory for employees. The Informant explained that this tool was for use in the PRC only, and none of its data was transferred abroad. Several Participants mentioned operating in-country only supply chain monitoring systems.

More recently, PRC data regulators have provided fresh guidance on cross-border data transfers in the form of the CAC Measures on Cross-border Transfers (most recently revised in 2024), which some Informants found helpful. It was noteworthy that some Participants considered concerns over PRC data legislation mostly settled and therefore a thing of the past, whereas other Participants flagged up the space as one of continuing and serious difficulty – with some knowingly operating in breach of the letter of the law (see below). It is possible that experiences diverge as a result of Participants' corporate profile, geography and scale of activities in the PRC.

One Participant compliance officer expressed what could be an emerging view among foreign companies in the PRC. Chamber of Commerce survey data provides some support in this regard.

"What is data? What is important data? These terms were not clearly defined until three to five years after the laws were put in place. Now I think we have reached a point where almost all these definitions are clear, very well defined. And now there are more people equipped with the legal and the IT knowledge who are capable of running compliance programmes."

iii. Lack of enforcement clarity

Several Participants pointed out that their providers of global enterprise systems were currently unable to supply PRC-compliant solutions. In particular, the cloud storage features of these systems would in most cases not offer an option for a domestic "PRC cloud", meaning data would by default be transferred cross-border, potentially in breach of PRC law.

Given how dominant some of these systems are in their respective sectors (as seems to be the case, for example, with certain HR management systems), Participants appeared to have formed the view that sudden, broad-based, PRC enforcement initiatives were unlikely. The ability to monitor and assess enforcement risk remains a critical skill, and several Informants discussed how they actively managed their exposure by staying in close contact with enforcement bodies.

"The head of the Cybersecurity Bureau is my classmate, so I have a very strong connection there. From time to time, I have discussions with them on how to handle this [challenges regarding data regulations], and they are very interested in this area."

Participant lawyer explaining the value of unofficial contacts.

Consequently, Participants find themselves in a state of limbo where the use of non-compliant systems continued without a clear roadmap towards full data compliance. Even when risk was assessed to be low, enforcement directed against noncompliant practices could never be completely ruled out. One Informant highlighted the need to appreciate the practice of “selective enforcement”, which implies that a Participant’s risk profile could increase as a result of external factors, such as sudden political developments involving the Participant’s Home Country.^x

“In the PRC, most of these enforcements are selective enforcements. Depending on the specific political situation, they choose different targets for enforcement.”

Inhouse lawyer discussing political dimension of risk assessment.

Several Participants reported that they had benefited from recent clarifications regarding the Personal Information Protection Law and Data Security Law. One Informant stated that their company was able to rely on one of the new exemptions to transfer data out of the PRC under a less stringent reporting structure. However, some Participants described this clarity as a double-edged sword; while it removed ambiguities, it could also present challenges if it led to stricter, explicit compliance requirements, meaning Participants might have to adjust processes that exploited grey zones previously in existence.-

Participants also reported challenges regarding PRC legislation on the use of data security tools, as well as inconsistent enforcement on their use. For example, one Participant noted the use of an encryption tool in cross-border transfers. PRC law generally requires encryption software to be registered with local cybersecurity authorities; however, these authorities were found to be unaware of the requirement. When the Participant insisted on reporting usage according to law, the authority asked for the encryption key. This would have compromised the Participant’s encryption system and, according to the Informant, was “out of the question”:

“So, the authority said, “Yeah, yeah, that’s what the law requires, but you’re the first one in 10 years” but we still went through with it. Maybe we were just stupid. We read the law. We find it’s relevant. Then we try to follow it.”

In-house lawyer describing how an ambitious compliance programme may run into unexpected practical challenges.

In the end, the requirement was deemed to have been fulfilled by Participant and authority alike simply by having the company explain the encryption system’s main features, without any disclosure that would allow the authority access to encrypted data.

e. Code of Conduct-driven Compliance Dilemmas

The interviews revealed that, while Participants had concerns about CSRD and CSDDD implementation (as noted above), these processes were institutionally managed and supported by central group functions. While several Participants indicated that comprehensive multi-tiered due diligence on supply chains in the PRC might not be feasible, none suggested that EU supply chain rules posed a long-term strategic challenge to their operations in the PRC.

By contrast, “traditional” compliance work aimed at managing the tension that exists between a Participant’s Code of Conduct derived from Home Country laws, international benchmarks in areas such as labour rights and environmental standards, as well Participant’s own ethics commitments, on the one hand, and Host Country legislation and policies, on the other, was keeping Informants as busy as ever. What is striking about this category of compliance dilemmas is that it often emerges as a result of Participants’ desire to go further with their compliance standards than is required by the law.

This section highlights the findings regarding Code of Conduct-driven compliance dilemmas using three mini case studies.¹⁰ It shows that Participants sometimes find themselves in situations where they struggle to implement Code of Conduct requirements that go beyond applicable legal demands.

i. Labour rights: Complexity around overtime working

Several Participants mentioned that they had formerly struggled with issues such child labour and illegal overtime in their PRC supply chains but that PRC workplaces and labour practices had since been modernised. Informants who had witnessed this trend seemed to sense that PRC workers, by and large, were no longer at risk of this type of exploitation in the manner that had once been the case.

Not all Informants shared this view, however, and one Participant shared how they were involved in a highly seasonal field that normally involves extensive overtime among PRC-based staff in peak season. The Informant noted that some local overtime practices observed among competitors appeared to be in breach of PRC labour law. The Participant’s Codes of Conduct, on the other hand, applied an even stricter standard based on regulations published by the International Labour Organisation. This meant that a Code of Conduct-based Compliance Dilemma arose.^{xi}

To complicate matters further, some local workers insisted on working as many hours as possible in peak season. There was a real risk of losing staff to competitors with less stringent Code of Conduct practices if they were not allowed to do so. In addition, there was a very real threat that a Participant’s adherence to shorter working hours might prevent orders from being fulfilled on time.

The Informant’s experience was that local authorities were not responsive to reports of companies breaching rules on overtime, and that their focus lay instead on promoting the local economy. In addition, the Informant had found that interest among international customers in compliance with labour rules was uneven, leading to major competitive challenges.

While some of the Participant’s customers recognised the Participant’s efforts to uphold its Code of Conduct, and were willing to pay a premium, others were prepared to drop the Participant as a supplier if they could not supply at the level of (in the Informant’s view) less scrupulous competitors.

¹⁰ Given the nature of the study, the case studies are anecdotal rather than necessarily typical for all, or even most, Nordic MNCs in China. The case studies were brought up spontaneously by Informants during the course of interviews and are included here as they highlight diverse categories of compliance challenges faced by Nordic MNCs in China.

"There are international customers who are more on our side, in that they choose us for a reason and they refuse to work with local competitors that have no respect for those [labour] laws. And then sometimes we even see international customers that don't work directly with the [first-tier] suppliers. They work with outsourced contractors, and then things get layered and there might also be corruption involved, so these illegal practices of our competitors never reach the customer."

Participant in-house lawyer commenting on the difficulty of implementing a Code of Conduct when some competitors are tempted to take shortcuts.

The Participant's challenges in this regard were ongoing and the Informant did not report having arrived at a satisfactory conclusion.

ii. Engaging consultants in grey zones

A conflict between the Code of Conduct and Host Country policies arose for a Participant that had for many years sought to resolve protracted issues related to land use. The Participant had been leasing land from a local government but learned over time that there were legacy claims to the land from local residents. The claimants referenced historical circumstances that were very difficult for the Participant to assess.

The Participant found itself being used for leverage in a land dispute that should not have been their direct concern. Nonetheless, third parties who were potentially affiliated with the land claimants mounted actions that disrupted the Participant's work on site. Moreover, threats were made to the Participant's employees and property.

At this point, the local government offered the services of an unofficial mediator with local standing. However, the Participant was unable to verify what methods would be used by this mediator, or to rule out bribery or threats. Since the person involved would have been an external contractor, the company saw no conflict with Home Country legislation as long as they conducted due diligence to the best of their ability. In this case, the primary conflict – leading to the Participant losing access to leased land – was between operational interests and the Code of Conduct, not Home Country or Host Country legislation. The Informant elaborated on how tempting it would have been for the Participant to accept such an offer, but how ultimately the inability to arrive at a reasonable level of Code of Conduct compliance forced it to decline.

"So, if I quote the UK Bribery Act, you can do all the "adequate procedures" and then you can claim, "look, we have done our homework to the extent allowed by local laws and we couldn't find anything". So there's a big temptation to hire that kind of a service, because in exchange you [solve your problem], which is a big operational expense. And then if we say that, well, with this big question mark and ambiguity, we just cannot use that service. And then the consequence of that is that [the problem remains unresolved], and that accumulates to millions of euros every year. So there the company faces a giant dilemma."

Participant in-house lawyer commenting on having declined an offer to use a local consultant to help resolve a long-standing operational challenge.

iii. Customer screening: Implementing Code of Conduct end-user restrictions in the PRC

Customer and end-user screening was widely practiced by Participants. This kind of screening might be driven by legal mandates in Home Country or Third Country legislation, as is the case with sanctions or rules on military end-users. It can also be driven by Codes of Conduct. For study Participants, this often concerned sales to Russian customers in the wake of Russia's 2022 full-scale invasion of Ukraine. Some Participants reported having Codes of Conduct that were stricter in this regard than required by EU or other international sanctions. Some Codes of Conduct contain blanket bans on any direct or indirect sales to Russian end-users. For Participants marketing and selling industrial products in the PRC, that requires close monitoring of the end-use of their products by PRC customers.

Participants reported complexities in tracking end-users in cases where PRC counterparts might re-sell products. Informants shared that this monitoring mostly takes the form of customers issuing end-user certifications. Participants acknowledged that a "good faith" procedure of this nature could be circumvented by a "bad faith" actor seeking to serve as an intermediary for onward sales to banned end-users. For this reason, site audits were undertaken on a selective basis. One Informant told us that their PRC customers have been understanding and pragmatic when it comes to Participants' need to implement Code of Conduct end-user restrictions.

"You have three production lines. That one is for Russia, and we only supply the other two. We find many private PRC companies are very pragmatic; they understand us and are willing to comply."

Participant in-house lawyer commenting on implementing end-user restrictions in the PRC.

3. Conclusions

This section addresses the research questions that prompted this study. The analysis attempts to draw on the experiences of the Participants and to articulate the themes that came up in the interviews. The conclusions are an initial vantage point for discussion of the compliance dilemmas within the Nordic MNC community and a reference point for future research.

a. Nordic MNC's experience of Compliance Dilemmas in the PRC

Nordic MNCs encounter four different types of compliance dilemma in the PRC, categorised as Pure, Home Country-driven, Host Country-driven and Code of Conduct-driven. The compliance dilemmas triggered by supply chain due diligence requirements and PRC data regulations, respectively, pose particular and deep-seated challenges.

Nordic MNCs that find themselves in pure compliance dilemmas are caught between conflicting legal regimes that are equally binding on the company. Wherever such a scenario materialises, the Nordic MNC faces significant legal risk. Considerable effort is therefore made to avoid such situations. For example, Nordic MNCs deploy elaborate strategies in relation to sanctioned counterparts. Such individuals or entities are “flagged” as part of routine know your customer (KYC) checks for the purpose of avoiding direct sanctions breaches. In addition, Nordic MNCs have developed “playbooks” on how to decline business in a manner that minimises the risk of triggering PRC Blocking Rules.

This study of compliance dilemmas was originally triggered by ongoing implementation of various EU directives with extraterritorial application, notably the CSRD and the CSDDD.

While these were consistently raised in surveys of the PRC's business climate as experienced by foreign companies, Nordic MNCs for the most part are relatively comfortable with ongoing and expected implementation efforts. This is in no small part thanks to the significant investment made by Nordic MNCs in global compliance programmes targeting emerging European corporate sustainability regimes.

There are still concerns, however, in particular when it comes to the ability of Nordic MNCs to access verifiable supply chain data in a PRC context.

Compliance dilemmas related to the PRC-based supply chains of Nordic MNCs also arise more broadly in the context of a company's own Code of Conduct, for example when it comes to countering fraud or implementing a company's ethical standards. Here, issues might relate to the often complex and idiosyncratic local terrain in which a Nordic MNC finds itself. Thus, there are no typical cases, but rather a broad range of challenges that can stem from issues such as uneven enforcement of labour laws, unclear land-use rights or the need for Nordic MNCs to implement global end-user restrictions.

“While these were consistently raised in surveys of the PRC's business climate as experienced by foreign companies, Nordic MNCs for the most part are relatively comfortable with ongoing and expected implementation efforts. This is in no small part thanks to the significant investment made by Nordic MNCs in global compliance programmes targeting emerging European corporate sustainability regimes.”

Among the compliance dilemmas driven by Host Country legislation, those that stem from the PRC's data laws dominate. Nordic MNCs must manage intricate challenges related to imprecise legal definitions of data deemed sensitive under PRC law, the limited mobility of PRC personal data, and a lack of clarity of enforcement around legislation as it stands. Nordic MNCs often find themselves operating in a PRC data legislation grey zone and deploy various strategies to manage associated risks.

b. What strategies do Nordic MNCs in the PRC employ to cope with Compliance Dilemmas?

MNCs respond to compliance dilemmas by applying strategies that are referred to in this report as coping mechanisms.^{xii} Common coping mechanisms include:

- (i) investment in compliance programmes to manage risk in a systematic fashion;
- (ii) restructuring operations within a group of companies to avoid or reduce exposure;
- (iii) policy and advocacy work to seek changes to relevant legislation; and
- (iv) exiting or reducing presence in a certain jurisdiction.

The main observations in this regard are highlighted below. The table in Appendix C summarises how Participants reported coping with different types of compliance dilemma.

i. Investment in compliance programmes

The compliance teams of Nordic MNCs comprise highly qualified officers, often with vast experience in the field. They constitute a carefully crafted first line of defence against compliance dilemmas. PRC-related compliance programmes are typically considered strategically significant in the headquarters of Nordic MNCs and senior compliance officers serve with or in the immediate proximity of senior executive leadership.

The work of compliance teams is not limited to policies and procedures, such as the launch and management of the MNC's Code of Conduct. It extends to important networking and liaison work, which is typically conducted by senior compliance officers in person. Thus, Nordic MNCs rely on the continuous building of relationships of trust – with PRC suppliers and authorities – combined with legal and structural arrangements to provide sufficient assurance of compliance. In this sense, the successful operation of a PRC compliance programme is as much craft as it is science for Nordic MNCs.

This also means that there is a “black box” element to how Nordic MNCs cope with compliance dilemmas in the PRC, leaving HQ potentially in the dark with respect to important strategic deliberations conducted between Nordic MNC's in-country staff members and their supplier and government interlocutors.

Within their in-country compliance operations, Nordic MNCs often rely on high-level PRC nationals who have developed key government and supplier relationships, often over decades, to gauge the level of risk related to non-compliance and the likelihood of enforcement. Compliance officers with such profiles can enable Nordic MNCs to engage with PRC local authorities to arrive at an agreed, negotiated approach that avoids the need for full compliance.

In contrast, SME coping mechanisms might be highly pragmatic and risk-based, reflecting their constrained resources. Rather than relying on formal systems, decisions are often made on a “best efforts” basis. As the study’s SME Informant noted, compliance responses are sometimes based on incomplete information and the company effectively *“replying to the best of our knowledge and hoping for the best”*.

At the same time, some areas of compliance work, in particular those related to supply chains, can over time be assisted by the PRC’s own developing legislation. One Informant referred to the PRC’s emerging Environment Social and Governance (ESG) requirements as a factor contributing to improved alignment between the practices of PRC suppliers and foreign due diligence regimes. Another Informant highlighted a cultural shift in the PRC in relation to workplace safety and the impact of industry on the environment, which they saw as partly a result of PRC companies having worked for decades with foreign customers.

ii. Structural adaptation

As cross-jurisdictional compliance issues have arisen, Nordic MNCs have increasingly taken a China-for-China approach to data management. Data that could potentially be classified as sensitive by the PRC authorities is not transferred across borders. Nordic MNC group level staff who no longer have access to this data are left to rely on internal assurance mechanisms that in-country staff are operating in line with Code of Conduct requirements.

When it comes to KYC work, this increased reliance on in-country staff and less than full transparency in group level compliance functions could jeopardise alignment of compliance practices across geographic regions for Nordic MNCs.

In scenarios where Nordic MNC group-level functions are no longer directly involved in in-country data management procedures, in-country staff members might be assuming unintended (and potentially severe) legal liability under PRC data and national security laws.

Across areas of compliance, Nordic MNCs adopt a risk-based approach to assurance. In the context of sanctions, Nordic MNCs are sometimes prepared to adopt creative (legal) workarounds to sanctions requirements. For example, to avoid both dealing with a sanctioned entity and contravening PRC Blocking Rules, Nordic MNCs might adjust production capacities or report an inability to fulfil an order due to “production line changes or strategic reorientation”. As part of their risk analysis, Nordic MNCs report detailed internal assessments of partners to review ownership structures, connections with the military and, at product component level, the substitutability of components (e.g. those of US origin).

In the context of structural adaptation, relationship building with key constituents, including both strategic suppliers and regulators, plays an important role. Sometimes, Participants

“This also means that there is a “black box” element to how Nordic MNCs cope with compliance dilemmas in the PRC, leaving HQ potentially in the dark with respect to important strategic deliberations conducted between Nordic MNC’s in-country staff members and their supplier and government interlocutors.”

“In scenarios where Nordic MNC group-level functions are no longer directly involved in in-country data management procedures, in-country staff members might be assuming unintended (and potentially severe) legal liability under PRC data and national security laws.”

were able to rely on a large first tier supplier as an intermediary in its broader relationship with a vast ecosystem of suppliers at lower tiers. For example, one Participant had a long-term relationship with an important first tier supplier, which it described as fostering mutual trust. In this context, the Participant would ask the first-tier supplier to provide data from underlying suppliers as needed. According to the Informant, the size of the first-tier supplier, along with its considerable resources and established processes, had over time built significant trust within the Participant's organisation.

Increased transparency and trust could sometimes be seen emanating from arrangements where representatives of the Participant spent considerable time seconded to supplier premises, for example in order to oversee technology transfer or quality control. One Informant spoke of how seconded staff could sometimes perform certain required data collection tasks that would otherwise have been requested from the secondment host.

iii. Policy and advocacy work

Nordic MNCs reported engagement through various channels, including Home Country governments, chambers of commerce and business networks, to voice their concerns. Efforts have concentrated on lobbying for adjustments to specific industry regulations and sought the optimisation or clarification of key standards or requirements that affect their competitive position, rather than to regulations that present compliance dilemmas.

Codes of Conduct and values play a key role in defining where lobbying is appropriate. Nordic MNCs generally seek to be at the forefront of the green transition and are therefore reluctant to get involved in lobbying efforts aimed at slowing down implementation of new rules and regulations in this area. While Nordic MNCs engage with chambers of commerce, embassies and business networks, they generally avoid employing external PR agencies for lobbying work aimed at ameliorating the impact of compliance dilemmas in the PRC.

Our Informants were typically not drawn from government affairs or other functions involved in lobbying work so findings in this area are therefore tentative. It was, however, quite clear that policy and advocacy work mostly play a supporting role in the overall compliance effort of Nordic MNCs.

iv. Exiting or reducing presence

While some version of China-for-China increasingly features in the compliance strategies of Nordic MNCs, this study found no examples of Nordic MNCs that have left or significantly reduced their presence in the PRC. Some Nordic MNCs have, however, moved or discontinued some elements of their PRC operations as they implement China-for-China strategies. Depending on the Nordic MNC's overall geographic focus, such strategies might entail a reduced presence in the PRC.

c. How significant is the impact of Compliance Dilemmas on the strategic objectives of Nordic MNCs?

Compliance dilemmas have implications for global strategy that, within a global risk-based approach to operations, mean that Nordic MNCs must continuously make strategic adjustments. Three themes stand out.

i. Nordic MNCs remain deeply invested in the PRC market

Nordic MNCs have to some extent shifted trade and sourcing patterns in response to political risk and the politicisation of supply chains. This has had a direct impact on PRC operations and many respondents report less manufacturing for export in the PRC. The PRC will remain – and potentially grow in significance as – a key destination for Nordic MNC sales, however, so it is unlikely that a significant proportion of companies will consider leaving the PRC in the foreseeable future.

In addition, cost advantages persist, and price – including the cost of compliance – continues to be a decisive factor in the strategic decision making of Nordic MNCs. More than one Nordic MNC pointed out that as challenging as PRC compliance work can be at times, **other markets where the company is active present their own sets of equally tricky – and costly – compliance dilemmas.**

ii. China for China is a clear trend

The bifurcation of global supply chains between the PRC and rest of the world is an ongoing trend with many nuances. Nordic MNCs appear to be taking a flexible approach to China-for-China, in that they are not categorically severing links with the PRC across their supply chains, but frequently refer to the concept in the context of global risk and compliance management. For some Nordic MNCs, flexibility is the key. They maintain a significant global production footprint in the PRC but are prepared for contingencies should this need to be shifted elsewhere in short order.

While changes in global manufacturing patterns are an important driver, some PRC-specific challenges, for example with data compliance, also contribute to an accelerating shift to more of a China for China model among Nordic MNCs. In other words, it is not only Nordic MNC

supply chains that could end up bifurcated. Related internal company operations, such as compliance programmes, may also be divided into separate silos for the PRC and the rest of the world. Several Nordic MNCs are aware of this and maintain an impressive level of global oversight at HQ.

"Nonetheless, the challenges associated with overseeing increasingly disjointed compliance operations should not be underestimated."

Nonetheless, the challenges associated with overseeing increasingly disjointed compliance operations should not be underestimated.

iii. The Growing Impact of Compliance Dilemmas

Nordic MNCs report spending ever more time and resources on compliance dilemmas related to their PRC operations. While some company officers express frustration over the seemingly never-ending stream of rules and regulations, it is clear that the issue is not going to go away.

Given how Nordic MNCs continue to view the PRC as a key market in their global strategies, and how the PRC increasingly poses a unique set of compliance challenges, many companies view the development of in-house PRC compliance know-how as particularly valuable. The competitive edge this may represent is underlined by the "craft" (as opposed to "science") aspects of the compliance work performed by Nordic MNCs in the PRC that are highlighted in this study.

4. Recommendations

Even within the limited sample of this study, there are considerable variations in the analyses and approaches of Nordic MNCs to similar circumstances. While some variance is to be expected, there is room for more dialogue within the business community aimed at establishing best practices among Nordic MNCs with respect to the compliance dilemmas encountered in the PRC. By the same token, continued engagement on the topic of corporate compliance between business, on the one hand, and policymakers and analysts, on the other, would contribute to an even better informed approach to policymaking and a more nuanced tone in bilateral discussions. Our main recommendations are:

- Adjust Nordic MNC corporate risk models to reflect the fact that supply chains are increasingly viewed through a national security lens
 - The PRC has brought supply chain security and governance formally within its national security framework while the European Union, which has no national security competence, has arrived at a functionally similar position through the language of economic security and resilience. As a result, companies are increasingly obliged to gather information about their suppliers that some jurisdictions, notably the PRC, now restrict them from asking. Traditional strategies, such as those aimed at “exploiting” grey zones or those based on a low likelihood of enforcement, may no longer be viable. Similarly, **assuming that enforcement will continue to be absent is an increasingly risky strategy.**
- Renew and intensify dialogue between the worlds of government and business on the topic of corporate compliance
 - This study has identified serious concerns – and significant untapped potential – when it comes to the management of compliance dilemmas in a PRC setting. **Nordic MNCs could better harness the close and informal connections that traditionally exist between policymakers and corporate boards** in the Nordic countries. Where there is a will, new initiatives could get off the ground quite easily.
- Proactively review and address the hidden compliance risks in relationships between Nordic MNC headquarters and in-country operations
 - Implementation of China-for-China strategies means that in-country teams are increasingly left to handle complex compliance environments on their own. This creates uncertainty from a global compliance management perspective. In addition, the legal exposure of in-country staff is not always properly assessed.
 - Nordic MNCs should thoroughly review the potential impacts on global operations and take a pragmatic approach to communicating this with governments. In particular, **Home Country governments should be sensitised to the severe nature of certain compliance dilemmas and the ways in which they impact business.**

- Strengthen the compliance capabilities of SMEs
 - The limited resources typically available to SMEs in the face of a complex regulatory environment means that they are often the weakest link when new compliance legislation, such as the CSRD or the CSDDD, is implemented. **Policymakers need to consider how to advance the goals of new legislation without squeezing SMEs.** There is also room for initiatives within the business community that can put SMEs in a better position to respond to the requirements of their larger corporate peers.
- Consider whether business-led compliance initiatives might prove a more cost-efficient pathway than legislation for achieving policy goals
 - This study has highlighted how Nordic MNCs, through their Codes of Conduct, chart their own course towards objectives that are often more ambitious than those imposed by binding legislation
 - The question therefore arises whether there is room for closer alignment of government policy goals and initiatives that would be undertaken by the business community without the need for legislation ^{xiii}
 - Given the trend for China-for-China highlighted in this study, the question needs to be asked whether the EU supply chain directives, which aim to spread European supply chain compliance practices globally, are in fact having the opposite effect ^{xiv}
- Sharpen the competitive edge of Nordic MNCs when it comes to coping with compliance dilemmas in the PRC
 - Expertise has been built by combining rigorous policies and procedures, which as per company Codes of Conduct can be more demanding than applicable law, with a mandate for responsible officers to apply these with discretion in the PRC operating environment (the “craft” side of compliance work) .
 - Many Nordic MNCs possess unique know-how on coping with compliance dilemmas. There is a need to increase knowledge sharing among industries and companies for the benefit of Nordic business in the PRC as a whole.
- Build on this study to conduct further research into compliance dilemmas in a PRC setting
 - As more companies share their own unique experience, the collective base of knowledge will expand for the benefit of the business and policy communities
 - The four types of compliance dilemma used in this analysis could fail to capture important aspects of the challenges faced by Nordic MNCs and should be further scrutinised within an expanded study
 - Questions directly related to compliance dilemmas could be inserted into business climate surveys conducted by chambers of commerce in order to build a base of quantitative data on the topic
 - Further initiatives should be encouraged, in the mould of this study, that bring together a set of Nordic PRC researchers from different backgrounds.

**Kristian Odebjer (Project Director)**

Kristian Odebjer is a lawyer admitted in Sweden and Hong Kong. He is a Consultant with Hong Kong law firm Boase Cohen & Collins.

**Kevin Broady**

Kevin Broady is the Chief Analyst at the China Office of Finnish Industries.

**Anton Karppanen**

Anton Karppanen is an Analyst at the China Office of Finnish Industries

**Helena Löfgren**

Helena Löfgren is an Analyst at the Swedish National China Centre.

About the China Office of Finnish Industries

The China Office of Finnish Industries Oy (CoFI) is a nonprofit company established to provide independent analysis on the People's Republic of China (PRC) to 25 Finnish multinationals with a strategic interest in the PRC. CoFI is a private limited liability company based in Helsinki, Finland, and funded by its shareholders.

About the Swedish National China Centre

The Swedish National China Centre (NKK) was established in 2021 as an independent unit at the Swedish Institute of International Affairs (UI). The Centre conducts policy-relevant research and aims to contribute to a long-term improvement in the state of China-related knowledge in Sweden. UI's publications undergo internal quality control. Any views expressed are those of the authors.

Appendix A Laws at the Root of PRC Foreign Compliance Dilemmas: A sample ^{xv}

PRC Legislation

Set of Rules	Short Name	Year Enacted	Regulatory Context	Compliance Dilemmas
Provisions on the Unreliable Entity List (中华人民共和国不可靠实体清单规定)	UEL	2020	Creates a mechanism allowing China to designate foreign entities that endanger national sovereignty, security, or development interests.	- If Ministry of Commerce (MOFCOM) prohibits transactions with a listed entity, continuing to transact would violate binding administrative measures. - The Provisions allow MOFCOM to conduct investigations, request materials, and require explanations; entities under investigation must cooperate.
Rules on Counteracting Unjustified Extraterritorial Application of Foreign Legislation and Other Measures (阻断外国法律与措施不当域外适用办法)	PRC Blocking Rules	2021	China's "Blocking Rules" — mechanism to counter certain foreign extraterritorial laws.	- Where a foreign law or measure prohibits or restricts a Chinese citizen, legal person, or other organization from engaging in normal economic, trade or related activities with a third state (or its citizens/organizations), the affected Chinese party must truthfully report the matter to MOFCOM within 30 days. ("Chinese legal person" includes subsidiaries of foreign companies established in China.) - If MOFCOM determines the foreign measure constitutes unjustified extraterritorial application, it may issue a prohibition order. Relevant parties shall not recognize, enforce, or comply with that foreign measure. - If a party suffers losses because another party complies with a prohibited foreign measure, the injured party may bring suit in Chinese court.
Anti Foreign Sanctions Law of the People's Republic of China (中华人民共和国反外国制裁法)	AFSL	2021	Framework law authorizing countermeasures against foreign sanctions.	- Provides that no organization or individual shall implement or assist in implementing discriminatory restrictive measures imposed by foreign states against Chinese citizens or organizations. Violations may trigger countermeasures or civil liability. - If a countermeasure list is issued and a company continues transactions prohibited by the measure, the company could face asset freezes and become subject to transaction prohibitions.
Provisions of the State Council on the Security of Industrial and Supply Chains (国务院关于产业链供应链安全的规定)	Decree No. 834	2026	The first dedicated national regulation focused specifically on industrial and supply chain security	- Empowers authorities to launch investigations against countries, regions, or entities that impose discriminatory restrictions affecting China's industrial and supply chains. - The Regulation allows the government to impose countermeasures, including restrictions involving trade, investment, technology, and data flows.

Regulation of the PRC on Countering Foreign States' Improper / Unlawful Extraterritorial Jurisdiction (中华人民共和国反外国不当域外管辖条例)	Decree No. 835	2026	Formalizes China's response framework to foreign sanctions, extraterritorial export controls, blocking-type legislation, and secondary sanctions	- Allows the State Council to identify "improper" foreign measures - Authorizes public prohibitions on compliance - Enables placement of entities on sanction lists - Allows inspections and enforcement actions, and - Introduces potential criminal liability.
Law of the People's Republic of China on Guarding State Secrets (中华人民共和国保守国家秘密法)	State Secrets Law	1988 (latest revisions in 2024)	Core national security legislation	- "State secrets" are defined as matters that concern national security and interests and are classified according to statutory procedures as "Top Secret", "Secret", or "Confidential". - In practice, state secret classification may not be transparent and could potentially be applied retroactively. - Handling of state secrets is subject to strict secrecy controls and unauthorized disclosure could trigger criminal liability. - Potential overlap between "state secrets" and (unclassified) "important data" designation under Data Security Law. - "National security" has (in other legislation) been widened to include economic security, technological security, supply chain security, financial security, data security, and resource security.
Counter Espionage Law of the People's Republic of China (中华人民共和国反间谍法)	Counter Espionage Law	2014 (latest revisions 2023)	Core national security legislation	- Prohibits stealing, spying, buying, or illegally providing "documents, data, materials, or items related to national security and interests." - 2023 revision expanded coverage beyond formal "state secrets" to include "data, materials, items related to national security." - The law provides that organizations and individuals have a duty to safeguard national security. Conduct that unlawfully acquires or transmits national-security-related materials may trigger administrative or criminal liability. - The law provides that "entities must assist state security authorities if required." Failure to cooperate can result in administrative penalties, detention, and potential criminal exposure.
Foreign Relations Law of the People's Republic of China (中华人民共和国对外关系法)	Foreign Relations Law	2023	National framework law	- The law affirms that China may take countermeasures where foreign acts endanger sovereignty, interfere in internal affairs, or harm national security or development interests.
Cybersecurity Law of the People's Republic of China (中华人民共和国网络安全法)	CSL	2017	Core cyber and data legislation	- Introduces mandatory safety protocols to widely defined "network operators". Failure to meet requirements may result in fines, rectification orders, business suspension, revocation of permits, and personal liability for responsible managers. - Significantly more demanding regime for organizations designated as operators of "Critical Information Infrastructure", including obligation to store personal information and "important data" in China and to conduct annual security evaluations.

Data Security Law of the People's Republic of China (中华人民共和国数据安全法)	DSL	2021	Core cyber and data legislation	- Applies to data processing, which is widely defined to include collection, storage, use, processing, transmission, provision, and disclosure of data. Means that companies maintaining HR systems, operating ERP systems, conducting analytics, or running R&D databases are covered. - Establishes internal management protocol and technical safeguards. - Companies found to be in breach are subject to fines, business suspension, revocation of permits, and personal liability for responsible persons. - Data categorized in tiers, namely "ordinary data", "important data", and "core state data". Conceptually parallel to state secrets system under State Secrets Law, but not necessarily applied in the same manner. Data categorization (unlike state secrets) does not depend on official classification. - "Important data" defined as "data that, if tampered with, destroyed, leaked, illegally obtained or used, may endanger national security, economic operation, social stability, public health and safety". - Organizations processing "important data" must designate responsible personnel, conduct regular risk assessments, submit risk assessment reports to regulators, and strengthen technical protections. Furthermore, government security assessment may be required for export of "important data". - Organizations in China may not provide data stored in China to foreign judicial or law enforcement authorities without approval of competent Chinese authorities.
Personal Information Protection Law (中华人民共和国个人信息保护法)	PIPL	2021	Core cyber and data legislation	- The Chinese equivalent of EU's GDPR, with detailed provisions regarding the processing of personal data. - Cross-border transfer of personal information requires CAC security assessment, certification of accredited body, standard contract, or other lawful mechanism. - DSL "important data" restrictions still apply within context of PIPL. - Obligation for companies to appoint Personal Information Protection Officer. - Fines of up to 5% of annual revenue for company found in breach.
Measures for Security Assessment of Cross-Border Data Transfer (数据出境安全评估办法)	CAC Measures on Cross-border Transfers	2022 (latest revisions in 2024)	Detailed rules related to CSL and DSL provisions on data export	- Requires government security assessment for the export of "important data" or for export of large volumes of personal data (thresholds defined). - Approaches such exports as a national security issue (not "merely" a privacy issue). - 2024 "relaxation measures" lowered thresholds for personal information exports and created exemptions for certain routine business scenarios (but did not eliminate export assessment requirement whenever "important data" is involved).

EU Legislation

Set of Rules	Short Name	Year Enacted	Regulatory Context	Compliance Dilemmas
Corporate Sustainability Due Diligence Directive	CSDDD	2024 (with 2025-26 "Omnibus" amendment narrowing scope, easing requirements, and delaying implementation)	The Directive requires large EU and certain non-EU companies operating in the EU to conduct due diligence to identify, prevent, mitigate and remedy human rights and environmental harms in their own operations and across value chains.	Provides for - Mandatory risk-based due diligence - Civil liability mechanisms at member state level (fines may go up to 3% of net worldwide turnover) - Applies to companies with 5,000+ employees and EUR1.5 billion+ turnover (Omnibus) - Binding on companies from 2029
Corporate Sustainability Reporting Directive	CSRD	2022 (with 2025-26 "Omnibus" amendment narrowing scope, easing requirements, and delaying implementation)	The Directive requires companies to disclose standardized information about their environmental, social, and governance (ESG) impacts and risks.	Provides for - Environmental reporting (climate change risk, pollution, water and biodiversity impacts) - Social reporting (workforce conditions, human rights, supply chain impacts) - Governance reporting (business ethics, anti-corruption, risk management systems) - "Double materiality": reports to cover (i) how sustainability issues affect the company, and (ii) how the company affects people and the environment - Mandatory reporting for companies with 1,000+ employees and EUR450 million+ turnover - Implementation in process (depending on company size)
Carbon Border Adjustment Mechanism	CBAM	2023	Applies a carbon price to certain imported goods so that they face a cost equivalent to what EU producers pay under the EU Emissions Trading System.	- Importers of covered products (including cement, iron and steel, aluminium, fertilisers, electricity, and hydrogen) must report embedded emissions - "Carbon leakage" avoided through the mandatory purchase and surrender of CBAM certificates

Deforestation Regulation	EUDR	2023	Prohibits placing certain commodities and products on the EU market unless they are "deforestation-free", produced in accordance with relevant laws of the country of production, and covered by a due diligence statement	Before placing products on the EU market or exporting them, companies must: - Collect detailed information (including geolocation coordinates of production plots) - Conduct a risk assessment (including country risk level) - Mitigate any non-negligible risk - Submit a due diligence statement through the EU information system.
Forced Labour Regulation	FLR	2024	Will begin to apply in December, 2027. Introduces a prohibition on the placing and making available on, or exporting from, the EU market products made with forced labour at any stage of production	The prohibition applies to all economic operators, including non-EU entities - Forced labour is defined, in line with the ILO Forced Labour Convention, as "all work or service that is exacted from a person under coercion and for which the person has not offered themselves voluntarily" - Covers privately imposed forced labour, state-imposed forced labour and forced child labour - The law is enforced via an investigation process. Robust due diligence on forced labour will constitute a key defence strategy for companies targeted by investigations. This effectively means that many companies will have to tighten their compliance procedures with respect to forced labour

US Legislation

Set of Rules	Short Name	Type of Legislation	Year Enacted	Legal Force	Regulatory Context	Compliance Dilemmas
US export control legislation	US Export Controls	US Federal Law	1949 (and onwards)	Law with extraterritorial aspects	Export control legislation, most recently the Export Control Reform Act (ECRA) of 2018, and its associated Export Administration Regulations, gives the Bureau of Industry and Security (BIS), which operates under the Department of Commerce, the power to maintain an "Entity List".	- If a counterparty is listed on the Entity List, BIS license is required for the export, reexport, or transfer of most US origin items to the listed entity. - License requirement applies to US and non-US entities alike. - ECRA goes beyond traditional "entity" based restrictions by introducing additional export restrictions on semiconductors and other "emerging and foundational technologies".

US sanctions legislation	US Sanctions	US Federal Law	1977 (and onwards)	Law with extraterritorial aspects	The US International Emergency Economic Powers (IEEPA) Act of 1977 gives the President the power to declare a national emergency in response to any "unusual and extraordinary threat" to US national security, foreign policy, or economy, which largely comes from outside the country . Once that emergency is declared, IEEPA grants the President broad authority to investigate, block, prohibit, or regulate transactions involving property in which a foreign country or national has an interest.	- Sanctions manifested, for example, in the Specially Designated Nationals (SDN) list of individuals and entities with whom US persons may not trade (so called "primary sanctions") - Subject to further US legislation, SDN listing may also entail "secondary sanctions", whereby non-US persons may be penalized for doing business with sanctioned party
Uyghur Forced Labor Prevention Act	UFLPA	US Federal Law	2021	Law applicable to companies placing products on US market Extraterritorial elements	Creates a rebuttable presumption that goods made wholly or in part in China's Xinjiang Uyghur Autonomous Region are produced with forced labor — and are therefore prohibited from entering the United States.	Companies need to overcome a high burden of proof in order to "rebut" presumption. Unless importer can prove absence of forced labour, goods will be detained at US border and possibly seized.

Appendix B How do companies structure their PRC compliance operations?

i. Organisation

The structure and precise areas of responsibility of compliance teams varied widely between Participants. It appears that company size and global distribution of operations, as well as field of operations and complexity of supplier and client networks all play a part in determining how Participants choose to design their compliance structures. Participants used a combination of descriptors, such as “legal”, “compliance” and “ethics”, for the relevant teams; these names also influenced how teams saw their responsibilities and how these were delegated.

Informants included in-house lawyers, compliance officers, data security officers, sustainability officers and even CEOs. Some of the Informants were based in the PRC, others in the Nordics. It became clear during the course of the interviews that most officers in the compliance field truly believe that their work makes a difference. This commitment to the task tends to contribute to their professionalism and overall constructive approach to the various compliance challenges faced by Nordic MNCs in the PRC.

ii. Centrally managed function

Responsibility for compliance matters ultimately lies with the central group functions of Participants, notably at their Nordic headquarters. Compliance work is an increasingly critical strategic consideration and active sign-off by top management is required on certain compliance documents, such as corporate reporting drawn up under the CSRD.

Policies are drawn up at HQ and the Participant's Code of Conduct serves as the main reference in day-to-day operations. Participants rely on distributed teams in geographic and functional divisions for implementation of the Code of Conduct in business operations.

ii. Team size and reporting lines

The size of PRC-based compliance teams ranged from Participants with no designated compliance staff in the PRC, to a common set-up of one or two compliance officers in-country, to an upper range of six or seven compliance officers in the PRC in the case of one of the largest Participants. Participants with no designated compliance staff in the country rely on the country head or other senior officers to report on compliance matters to central group functions. Generally, companies with extensive in-country supply chains, and customer and distribution networks possessed larger PRC-based legal and compliance teams. Naturally, the size of compliance team also depends on the overall size of the Participant.

The experience of the SME Participant deviates significantly from this model. Without dedicated compliance personnel, responsibilities are distributed across existing roles. As the SME Participant's Informant commented, *“I don't have the resources to have one person working on this full-time”*. This illustrates how compliance functions in SMEs are embedded in broader operational roles.

iv. Role of compliance teams

Participants distinguished between the “proactive” and “reactive” activities of compliance teams, where the former refers to culture building and coaching (one Informant noted how in their “Ethics and Compliance Department”, *ethics* comes before *compliance*), and the latter refers to providing advice to internal stakeholders and investigating reported compliance shortcomings or breaches. In an example of proactive work, one Participant had been tracking the CSDDD for an extended period as they prepared for its implementation. Different aspects of compliance work are often separated into several teams, for example with one team covering supply chain compliance, another team covering anti-corruption and competition law, and a third team responsible for data compliance matters.

Despite the breadth of responsibilities covered by Informants, a slight majority were based in a legal or compliance department. Several of these lawyer Informants had a high level of familiarity with those aspects of compliance work that fell outside of their formal area of responsibility. This was sometimes related to their having previously served in another role but at other times it was related to the coordinating function of the legal department when it comes linking different areas of a Participant’s compliance work. In several cases, this broad personal perspective of a Participant’s compliance work seemed more than anything to stem from a desire on the part of the individual Informant to obtain as good a grasp as possible of the Participant’s risk profile.

Participants had often nurtured legal and compliance talent in the PRC for an extended period, allowing certain individual team members to become carriers of the group compliance culture. In several cases, Participants had taken organisational measures to provide HQ with direct access to such “field expertise”. From the multi-faceted compliance perspectives that these individuals shared in interviews, it appears that they were contributing considerable value to their companies. It is worth noting that legislation like the CSDDD emphasises a holistic approach to compliance work.¹

v. External support

While compliance work is sensitive and often concerns issues of a confidential nature, Participants occasionally involved outside parties, typically in the form of consultants, to assist with specific aspects of supply chain management, such as second- and third-tier supplier reviews. Outside lawyers are retained regularly by Participants to advise “proactively” on legal developments in the PRC. There was little evidence of outside lawyers routinely being involved in Participants’ “reactive” compliance investigations. By and large, these were left to be handled by in-house teams. Exceptions are made for particularly sensitive internal investigations, where “information control” is a concern and trusted outside counsel can be relied on to ensure the integrity of any information handled.

Participants also engaged with Home Country governments, as well as chambers of commerce and business networks (typically, but not exclusively, in the Host Country) to voice concerns over compliance issues more broadly, and sometimes in order to lobby for adjustments to specific industry regulations or to seek clarification of key standards or requirements that affect their competitive position.

¹ See for example the reference in Art.10 of the CSDDD to how “overall strategies and operations” should be designed to prevent the types of adverse environmental and human rights impacts targeted by the CSDDD.

vi. Informal networks

Several Participants reported how informal networks play a crucial role in their PRC compliance work. Participants highlighted how relationships with government representatives built up over time, sometimes going back to an Informant's student days, are of great value when assessing a Participant's exposure to enforcement action in a given compliance area.

"The connection with local government enables us to have very open dialogue about the concerns we have when it comes to [for example] the investment environment and Tax Authority probing into our high-tech status. I think we get very good support from the local government. I've never experienced the government refusing to provide guidance. Even if they do not know the answer, they will be able to connect you with the relevant department that can help."

Participant in-house lawyer commenting on the use of informal networks.

This modus operandi is sometimes considered part and parcel of how the PRC operates, but it also poses important questions for Participants, such as whether business secrets and confidential information more broadly risk being compromised when issues that may be of strategic significance are dealt with outside the scope of a company's normal operating procedures, and whether global business objectives can still be managed transparently within a company when parts of the PRC operation are dealt with within a "black box" of the undocumented personal network of a local employee.

Appendix C Coping Mechanisms: Summary Table

Type of Compliance Dilemma	Definition	Example(s) from Report	Coping Mechanisms	Real Examples from Interviews
Pure Compliance Dilemmas	Home/Third Country legislation clearly mandates Action X; Host Country legislation clearly prohibits it — Participant risks breach either way.	Home/Third Country secondary sanctions vs. PRC Blocking Rules (e.g. bans on sales to sanctioned Chinese entities)	Institutionalised sanctions monitoring (KYC checks, screening software) Avoid individual transactions or entire customer relationships Decline transactions citing commercial (not sanctions) reasons Redo bidding criteria / rework supply chains to exclude sanctioned parties Discontinue product lines carrying high sanctions exposure	Declined a transaction citing commercial reasons, handled “behind the scenes” New bidding round with modified criteria to exclude a sanctioned supplier Discontinued a Europe-made product line over Xinjiang-related exposure “China-for-China” design (no US tech) to stay compliant while still serving China
Home Country Driven Compliance Dilemmas	Home Country law mandates Action X; Host Country environment makes it (i) hard to implement or (ii) unpredictable in consequence.	CSRD (sustainability reporting), CSDDD (supply-chain diligence), EU Deforestation Regulation (wood-product companies)	Risk-based diligence — in-depth vetting of first-tier / strategic suppliers Supplier self-certification + proprietary risk-scoring frameworks Lean on long-standing supplier relationships for new reporting demands Accept some irreducible data uncertainty (pragmatic sign-off)	Long-standing supplier ties eased the CSRD reporting rollout SME Participant signed diligence forms despite inability to verify data (“crossing my fingers”) Small second-tier supplier of a hard-to-substitute part flagged for in-depth vetting
Host Country Driven Compliance Dilemmas (Chinese Data Legislation)	Host Country law prohibits Action X, which Home/Third Country doesn’t require but Participant wants to do anyway.	“Important/national core data”, personal data transfers (PIPL, DSL), cloud/IT localisation, state-secret-adjacent data	Keep sensitive data in-country (“China-only” systems) Use GDPR as an internal benchmark, despite no PRC legal validity Chinese legal advice / external law-firm risk mapping Informal contact with enforcement bodies to gauge “selective enforcement” risk Rely on CAC Cross-Border Transfer exemptions where applicable Training & access controls for state-secret-level data; supplier ownership arrangements to enable document transfer	In-house conflict-of-interest tool kept China-only, no cross-border transfer Encryption tool: registered despite being “first in 10 years”; satisfied regulator by explaining features without disclosing the key Informal tie to local Cybersecurity Bureau head (former classmate) for guidance Supplier-owned office located in Home Country to enable documentation transfer
CoC Driven Compliance Dilemmas	Participant’s own CoC sets a stricter standard than the law requires; Host Country conditions make that standard hard to implement or unpredictable.	Overtime limits stricter than Chinese law (ILO-based), anti-corruption exposure via “gray zone consultant”, end-user restrictions beyond legal sanctions (e.g. Russia)	Accept competitive disadvantage / lost orders rather than lower the CoC bar Segment customers — some pay a premium for compliance, others are lost Decline unverifiable “gray zone” fixes despite the cost Customer/end-user certifications + selective on-site audits Segregate production lines by destination market	Overtime: some customers paid a premium for CoC compliance; others switched to less scrupulous suppliers Land-use dispute: declined “gray zone consultant” despite millions/year in unresolved costs, given unverifiable bribery risk Russia restrictions: Chinese customers ran separate production lines per market, complying pragmatically
Cross-Cutting Coping Strategies (Conclusions)	Not tied to one dilemma type.	—	Investment in compliance programmes (staffing, systems, HQ priority) Structural adaptation (“China-for-China” restructuring of data/supply chains) Policy and advocacy work (chambers of commerce, embassies, business networks) Exiting/reducing presence (rare — no Participant has done this to date)	High-level PRC national staff with long-standing ties gauge enforcement risk “China-for-China” data kept in-country; HQ relies on local staff assurance Partner due diligence on ownership, military links, component substitutability Chamber/embassy engagement for regulatory clarification, limited direct lobbying

Endnotes

- i Li, J. (2024). Superpower Legal Rivalry and the Global Compliance Dilemma. *University of Pennsylvania Journal of International Law*, 891-951. <https://doi.org/10.58112/jil.45-4.2>
- ii For background discussion on what may be described as China's shift from a growth-oriented state capitalism to a "party-state capitalism" that prioritises political survival and risk management, see Pearson, M. M., Rithmire, M., & Tsai, K. S. (2022). China's party-state capitalism and international backlash: From interdependence to insecurity. *International Security*, 47(2), 135–176.
- iii The New York Times. (2021, April 6). Global Brands Find it Hard to Untangle Themselves from Xinjiang Cotton. *The New York Times*. Retrieved May 11, 2026, from <https://www.nytimes.com/2021/04/06/business/xinjiang-china-cotton-brands.html>; Bohman, V., & Pårup, H. (2022). Purchasing with the Party Chinese consumer boycotts of foreign companies, 2008–2021. Swedish National China Centre.
- iv For Companies in China, Pulling out of Xinjiang poses 'Messy Dilemma'. (2024, October 4). *The New York Times*. Retrieved May 11, 2026, from <https://www.nytimes.com/2024/10/04/business/china-xinjiang.html>
- v European Union Chamber of Commerce in China. (2025). European Business in China Business Confidence Survey 2025. Retrieved May 11, 2026, from <https://www.europeanchamber.com.cn/en/publications-business-confidence-survey>; The American Chamber of Commerce in the People's Republic of China. (2026). China Business Climate Survey Report 2026. Retrieved May 11, 2026, from <https://www.amchamchina.org/china-business-climate-survey-report/>; Team Finland. (2025). Team Finland China Business Confidence Survey 2025. Retrieved May 16, 2026, from https://finlandabroad.fi/documents/384951/0/TF+Confidence+survey_Apr25_Final_report.pdf/27c86569-beca-9310-f8a4-5bbb7dbad04b?t=1744185031470; Team Sweden. (2025). Business Climate Survey for Swedish Companies in Mainland China 2025. Retrieved May 11, 2026, from <https://www.swedcham.cn/business-climate-survey>
- vi Xi's Warm Words Jar With Reality for Foreign Companies in China. (2023, November 17). *Bloomberg News*. Retrieved May 11, 2026, from <https://www.bloomberg.com/news/articles/2023-11-17/xi-s-warm-words-jar-with-reality-for-foreign-companies-in-china>
- vii See for example page 15 of European Union Chamber of Commerce in China. (2024). European Business in China Position Paper 2024/2025. Retrieved from https://www.europeanchamber.com.cn/en/publications-archive/1269/European_Business_in_China_Position_Paper_2024_2025
- viii See for example European Business Organisation Worldwide Network. (2024). European Union Corporate Sustainability Due Diligence Directive (CSDDD) Position Paper. Retrieved from <https://euccan.com/wp-content/uploads/2024/07/EBOWN-CSDDD-Position-Paper.pdf>
- ix According to the 15th five-year plan (published 2026), current focus areas of industrial policy include, among others, robotics, hydrogen energy, next-generation IT, new

energy, new materials, connected NEVs, biomedicine/biotech, medical devices, shipbuilding, new batteries and storage, 6G, and low-altitude economy; see further Boullenois, C., Black, M., & Caruso, A. (2026). China's Next-Generation Industrial Policy. Rhodium Group & U.S. Chamber of Commerce. Retrieved from <https://rhg.com/research/chinas-next-generation-industrial-policy/>

x For background on selective enforcement, see Bellanger, B., & Chen, B. (2013). Dealing with Legal Grey Areas (and Selective Enforcement) in China. *International In-house Counsel Journal*, 6(22), 1–14.

xi Overtime regulation is a complex aspect of labour law. In research, it has been pointed out that Chinese practices have fallen short of ILO standards, for example when it comes to granting compensatory rest in exchange for overtime work (i.e. employers should not only grant monetary compensation); see Zhang, W. (2023). *Achieving Decent Work in China: A Case Study of Decent Working Time*. Meijers-reeks. Leiden. Retrieved from <https://scholarlypublications.universiteitleiden.nl/handle/1887/3576738>

xii J. Li, 'Superpower Legal Rivalry and the Global Compliance Dilemma', *University of Pennsylvania Journal of International Law*, vol. 45 no. 4, 2024, p. 925.

xiii Representatives of Nordic industry have already urged the EU to manage regulatory gaps to reduce costs and risks for European companies in their China activities; see for example National Board of Trade Sweden (Kommerskollegium). (2026). Economic Security and Digital Trade: The Future of EU-China Data Flows. Retrieved from https://www.kommerskollegium.se/globalassets/publikationer/rapporter/2026/economic-security-and-digital-trade_the-future-of-eu-china-data-flows.pdf

xiv Analysis performed by the European Union Chamber of Commerce in China deserves to be revisited and expanded; see European Union Chamber of Commerce in China. (2024). Siloing and Diversification: One World, Two Systems. Retrieved from <https://www.europeanchamber.com.cn/cms/page/en/publications-siloing-diversification/426>; and European Union Chamber of Commerce in China. (2025). Dealing with Supply Chain Dependencies: Challenges and Choices. Retrieved from <https://www.europeanchamber.com.cn/cms/page/en/dealing-with-supply-chain-dependencies/441>

xv Wilmer Cutler Pickering Hale and Dorr LLP. (2016). China's Cybersecurity Law Imposes New Requirements on Doing Business in China. Retrieved from <https://www.wilmerhale.com/en/insights/client-alerts/2016-11-10-chinas-cybersecurity-law-imposes-new-requirements-on-doing-business-in-china>; Wilmer Cutler Pickering Hale and Dorr LLP. (2019). China's Unreliable Entity List. Retrieved from <https://www.wilmerhale.com/en/insights/client-alerts/20190729-chinas-unreliable-entity-list>; Wilmer Cutler Pickering Hale and Dorr LLP. (2020). China's MOFCOM Promulgated the Provisions on the Unreliable Entities List. Retrieved from <https://www.wilmerhale.com/en/insights/client-alerts/20200922-chinas-unreliable-entities-list>; Wilmer Cutler Pickering Hale and Dorr LLP. (2021). China Promulgates Data Security Law. Retrieved from <https://www.wilmerhale.com/en/insights/client-alerts/20210615-china-promulgates-data-security-law>; Wilmer Cutler Pickering Hale and Dorr LLP. (2021). China Enacts Anti-Sanctions Law. Retrieved from <https://www.wilmerhale.com/en/insights/client-alerts/20210611-china-enacts-anti-sanctions-law>; Wilmer Cutler Pickering Hale and Dorr LLP. (2021). China Issues Blocking Rules to Counter Secondary Sanctions. Retrieved from <https://www.wilmerhale.com/en/>

insights/client-alerts/20210121-china-issues-blocking-rules-to-counter-secondary-sanctions; Wilmer Cutler Pickering Hale and Dorr LLP. (2021). China Promulgates New Personal Information Protection Law. Retrieved from <https://www.wilmerhale.com/en/insights/client-alerts/20210830-china-promulgates-new-personal-information-protection-law>; Wilmer Cutler Pickering Hale and Dorr LLP. (2023). China Rolls Out Foreign Relations Law. Retrieved from <https://www.wilmerhale.com/en/insights/client-alerts/20230705-china-rolls-out-foreign-relations-law>; Wilmer Cutler Pickering Hale and Dorr LLP. (2024). China Finalizes Rules to Ease Data Export Compliance Burden. Retrieved from <https://www.wilmerhale.com/en/insights/client-alerts/20240326-china-finalizes-rules-to-ease-data-export-compliance-burden>; Wilmer Cutler Pickering Hale and Dorr LLP. (2024). China Revised the State Secrets Law. Retrieved from <https://www.wilmerhale.com/en/insights/client-alerts/20240326-china-finalizes-rules-to-ease-data-export-compliance-burden>; Wilmer Cutler Pickering Hale and Dorr LLP. (2024). MOFCOM Initiates Investigation into PVH Group Under China's Unreliable Entity List Regime. Retrieved from <https://www.wilmerhale.com/en/insights/client-alerts/20241014-mofcom-initiates-investigation-into-pvh-group-under-chinas-unreliable-entity-list-regime>