Downloaded from https://www.cambridge.org/core. IP address: 3.41.188.32, on 06 Nov 2026 at 13:18:20, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/err.2026.10151

European Journal of Risk Regulation (2026), 1–16
doi:10.1017/err.2026.10151

CAMBRIDGE UNIVERSITY PRESS

ARTICLE

When Compliance Infrastructure Becomes a Security Object: Legal Reclassification between EU Supply Chain Due Diligence and China's Order No. 834

Li Yuan

Faculty of Law, University of Helsinki, Finland
Email: li.yuan@helsinki.fi

Abstract

Supply chain law increasingly renders global production governable through compliance infrastructure: supplier mapping, audit rights, traceability records, risk scoring, geolocation data, contractual monitoring, digital platforms and cross-border evidence flows. This article argues that such infrastructure is no longer merely a technical means of implementing sustainability law. At the interface between European Union (EU) sustainability instruments and China's State Council Order No. 834, the same practice that appears as sustainability compliance in one legal order may be reclassified under another as security-relevant information gathering, discriminatory disruption or conduct affecting industrial and supply chain security. The article examines how compliance infrastructure can become a security object and identifies three connected sites of legal reclassification: evidence production, supplier leverage and evidence circulation. It contributes to risk regulation scholarship by directing attention from the content of compliance duties to the infrastructures through which those duties are performed and contested, while showing that Order No. 834 is better understood as a set of legality filters and escalation tools than as a blanket prohibition on EU sustainability compliance.

Keywords: compliance infrastructure; supply chain due diligence; supply chain security

I. Introduction

European Union (EU) sustainability law increasingly governs global value chains by requiring companies to know, document, and justify the conditions under which products enter the union market. Companies are no longer asked merely to publish high-level commitments. They must build systems that identify suppliers, trace products, assess risk, exercise leverage, store evidence, and explain decisions to regulators, customers, and, in some cases, courts.[1] The Corporate Sustainability Due Diligence Directive (CSDDD) gives this shift a general corporate form.[2] The EU Deforestation Regulation (EUDR) gives it a more concrete market-access form: covered products may not be placed on the Union market unless operators can support a due diligence statement with traceability and risk-

[1] J Salminen and M Rajavuori, "Transnational Sustainability Laws and the Regulation of Global Value Chains: Comparison and a Framework for Analysis" (2019) 26 Maastricht Journal of European and Comparative Law 602.

[2] Directive (EU) 2024/1760 of the European Parliament and of the Council of 13 June 2024 on corporate sustainability due diligence and amending Directive (EU) 2019/1937 and Regulation (EU) 2023/2859, OJ L, 2024/1760, 5.7.2024.

© The Author(s), 2026. Published by Cambridge University Press. This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (https://creativecommons.org/licenses/by/4.0/), which permits unrestricted re-use, distribution and reproduction, provided the original article is properly cited.

assessment evidence.[3] The EU Forced Labour Regulation (FLR) adds a complementary prohibition-based form by making supply chain and production information relevant to investigations and decisions concerning whether products made with forced labour may be placed or made available on, or exported from, the Union market.[4]

China's State Council Order No. 834, the Provisions on the Security of Industrial and Supply Chains, enters this landscape with a different vocabulary. It frames industrial and supply chains through security, resilience, controllability, risk monitoring, emergency response and countermeasures.[5] Its most relevant provisions do not simply prohibit foreign compliance systems. Article 13 addresses certain investigations and information-collection activities in China. Article 15 permits security investigations where foreign organisations or individuals interrupt normal transactions, adopt discriminatory measures, or otherwise cause or threaten substantial harm to the security of China's industrial and supply chains. Article 16 requires domestic organisations and individuals to comply with measures adopted under the security-investigation provisions and, where they fail to do so, allows further restrictions, including restrictions concerning data and personal information.[6]

The resulting problem is often described as one of regulatory conflict: Brussels asks firms to collect evidence and discipline suppliers, while Beijing may treat some of those acts as security-sensitive. That description is useful, but it does not go far enough. The deeper issue is legal reclassification. A supplier questionnaire, audit visit, satellite-linked plot record, termination clause, platform-generated risk score, or cross-border data transfer may move from one legal category to another as it crosses legal orders. In the EU setting, it may be compliance evidence. In the Chinese security setting, it may become information gathering, discriminatory disruption, data export or conduct relevant to supply chain security.

This article argues that compliance infrastructure has become a distinct object of legal analysis in contemporary supply chain law. By compliance infrastructure, I mean the organisational, contractual, digital and evidentiary systems through which obligations governing value chains become operational. These systems include supplier codes, contractual audit clauses, traceability files, certification schemes, due diligence platforms, escalation procedures, remediation plans, reporting templates and data-transfer channels. The central claim is that this infrastructure is no longer merely the background machinery of legal implementation. Under conditions of economic security, data sovereignty and sustainability regulation, compliance infrastructure can itself become a security object.

The argument is doctrinal and conceptual. It reads EU sustainability instruments and Order No. 834 as legal architectures for producing, moving, and controlling supply chain information. It does not claim that EU-style sustainability compliance is automatically unlawful in China, nor does it suggest that companies should retreat from human rights or environmental due diligence. The narrower claim is that compliance systems have become legally unstable because the features that give them operational strength also make them security-sensitive: visibility, traceability, standardisation, leverage and circulation.

[3] Regulation (EU) 2023/1115 of the European Parliament and of the Council of 31 May 2023 on the making available on the Union market and the export from the Union of certain commodities and products associated with deforestation and forest degradation and repealing Regulation (EU) No 995/2010 [2023] OJ L150/206.

[4] Regulation (EU) 2024/3015 of the European Parliament and of the Council of 27 November 2024 on prohibiting products made with forced labour on the Union market and amending Directive (EU) 2019/1937, OJ L, 2024/3015, 12.12.2024.

[5] State Council of the People's Republic of China, 国务院关于产业链供应链安全的规定 [Provisions of the State Council on the Security of Industrial and Supply Chains], State Council Order No. 834 (31 March 2026), English translation by China Law Translate <https://www.chinalawtranslate.com/en/-State-Council-Provisions-on-Industrial-and-Supply-Chain-Security/> (last accessed 26 June 2026).

[6] Ibid., Arts. 13, 15 and 16.

Downloaded from https://www.cambridge.org/core. IP address: 3.41.188.32, on 06 Nov 2026 at 13:18:20, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/err.2026.10151

The article therefore intervenes in a debate usually framed through extraterritoriality, private governance or business and human rights. These frames remain indispensable, but they do not fully capture the infrastructural form of contemporary supply chain regulation. EU law often governs foreign production through market access, private contracts and documentation rather than through direct commands to foreign suppliers.[7] The result is a form of regulatory projection that depends less on territorial jurisdiction in the classical sense than on the capacity to make non-EU production legible to EU-facing firms, platforms and authorities.[8] Once that legibility is produced through data-intensive systems, the same infrastructure becomes susceptible to a different legal description: not only as transparency, but as exposure; not only as accountability, but as extraction; not only as due diligence, but as a possible security event.

The article proceeds as follows. Part II situates the argument in the literatures on global value chains, mandatory due diligence, Chinese sustainable supply chain governance, private ordering, digital compliance and economic security. Part III explains how EU sustainability law operates as evidentiary infrastructure, focusing on the CSDDD, the EUDR, and the FLR. Part IV analyses Order No. 834 as a supply chain security filter rather than as a simple prohibition. Part V explains the selection and operation of three sites of legal reclassification. Part VI locates the article's contribution within existing infrastructural scholarship and draws implications for risk regulation, transnational private law, and compliance design. Part VII concludes.

II. From compliance duties to compliance infrastructure

The first strand of relevant literature concerns the legalisation of global value chains. Legal scholarship has shown that value chains are not simply economic facts waiting to be regulated. They are made legally visible through concepts such as lead firm, business relationship, chain of activities, market placement, contractual control and adequate governance. EU law is particularly important because it constructs global value chains differently across company law, consumer law, trade law and market regulation. Recent scholarship describes global value chains as regulatory proxies through which the EU transnationalises internal-market objectives beyond its territory.[9] Chinese legal scholarship has similarly examined how European and US supply chain legislation can produce extraterritorial effects through the control exercised by lead firms across global value chains.[10]

The second strand concerns mandatory human rights and environmental due diligence. Scholarship has traced the move from transparency and voluntary codes towards mandatory, risk-based due diligence in global value chains.[11] Chinese legal scholarship has likewise examined the transition from voluntary soft-law expectations to mandatory human rights due diligence, while questioning how far due diligence obligations should extend along supply chains and how their scope should reflect different relationships

[7] See A Bradford, *The Brussels Effect: How the European Union Rules the World* (Oxford University Press 2020).

[8] J Scott and L Rajamani, "EU Climate Change Unilateralism" (2012) 23 European Journal of International Law 469.

[9] A Beckers, "Global Value Chains in EU Law" (2023) 42 Yearbook of European Law 322; J Salminen, M Rajavuori and K Eller, "Global Value Chains as Regulatory Proxy: Transnationalising the Internal Market through EU Law" in A Beckers and others (eds), *The Foundations of European Transnational Private Law* (Hart/Bloomsbury 2024).

[10] Z Li, "欧美供应链法的扩张适用及其检视 [The Expanded Application of European and US Supply Chain Laws and Its Examination]" (2025) 9 (4) 武大国际法评论 [Wuhan University International Law Review] 55.

[11] M Wilhelm, "Mandatory Due Diligence Legislation: A Paradigm Shift for the Governance of Sustainability in Global Value Chains?" (2024) 7 Journal of International Business Policy 459.

Downloaded from https://www.cambridge.org/core. IP address: 3.41.188.32, on 06 Nov 2026 at 13:18:20, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/err.2026.10151

between firms and adverse impacts.[12] Chinese management scholarship adds a complementary operational perspective through sustainable supply chain management research on the coordination of environmental and social responsibilities across supplier networks.[13] The CSDDD has been analysed as a shift from disclosure towards the mandatory prevention of adverse impacts and as a hybrid instrument drawing on soft-law guidance, French vigilance law, German supply chain law, and EU sustainability policy,[14] while Chinese trade law scholarship has examined the Directive's regulatory pathway and the lessons it may offer for China.[15] Other work asks whether mandatory human rights due diligence can prevent abuses, create accountability and avoid becoming a process-centred exercise that benefits corporate risk management more than rightsholders.[16]

The transparency literature shows why this distinction matters. Disclosure and reporting regimes can improve visibility while still failing to change underlying conduct, especially when information is too aggregated, too technical, or too weakly connected to enforcement.[17] Studies of conflict-minerals reporting, modern slavery disclosure, and human rights reporting have repeatedly shown that information duties can produce elaborate documentary compliance without necessarily improving conditions for workers, communities or affected ecosystems.[18] Mandatory due diligence was partly a response to that limitation. Yet due diligence can reproduce the same weakness if the law rewards the existence of process more than the effectiveness of prevention, remedy and participation.[19] The infrastructure of compliance is therefore not normatively neutral: it may enable accountability, but it may also organise a legally defensible form of distance.

Recent risk regulation scholarship makes this point especially clear. Griffin and Fornasari argue that EU law increasingly uses corporate risk management obligations in both sustainability due diligence and digital platform regulation, entrusting large firms

[12] Y Tang, "强制性人权尽责立法的考量因素与类型化研究 [Research on the Considerations and Typology of Mandatory Human Rights Due Diligence Legislation]" (2024) 人权研究 [Human Rights Studies] 39; H Wang, "供应链人权尽责边界的比较分析与法理反思 [Comparative Analysis and Legal Reflection on the Boundaries of Supply-Chain Human Rights Due Diligence]" (2024) 人权 [Human Rights] 124.

[13] Q Zhu and F Wei, "动态环境下可持续供应链管理研究 [Research on Sustainable Supply Chain Management in a Dynamic Environment]" (2020) 1 供应链管理 [Supply Chain Management] 32; L Junjun, X Xiqiang and Z Qinghua, "新发展格局下的可持续供应链管理研究进展与展望 [The Research Progress and Prospects of Sustainable Supply Chain Management under the New Development Pattern]" (2025) 33 中国管理科学 [Chinese Journal of Management Science] 213.

[14] J Sinnig and D A Zetzsche, "The EU's Corporate Sustainability Due Diligence Directive: From Disclosure to Mandatory Prevention of Adverse Sustainability Impacts in Supply Chains" (2025) 16 European Journal of Risk Regulation 628.

[15] X Chen and W Shen, "欧盟《企业可持续尽职调查指令》：路径创新与中国借鉴 [The EU Corporate Sustainability Due Diligence Directive: Path Innovation and Lessons for China]" (2025) 国际贸易 [International Trade] 86.

[16] J Bonnitcha and R McCorquodale, "The Concept of 'Due Diligence' in the UN Guiding Principles on Business and Human Rights" (2017) 28 European Journal of International Law 899; C Mak, "Corporate Sustainability Due Diligence: More than Ticking the Boxes?" (2022) 29 Maastricht Journal of European and Comparative Law 301; S Deva, "Mandatory Human Rights Due Diligence Laws in Europe: A Mirage for Rightsholders?" (2023) 36 Leiden Journal of International Law 389.

[17] R Mares, "Corporate Transparency Laws: A Hollow Victory?" (2018) 36 Netherlands Quarterly of Human Rights 189.

[18] G Sarfaty, "Shining Light on Global Supply Chains" (2015) 56 Harvard International Law Journal 419; R Chambers and A Y Vastardis, "Human Rights Disclosure and Due Diligence Laws: The Role of Regulatory Oversight in Ensuring Corporate Accountability" (2021) 21 Chicago Journal of International Law 323.

[19] N Bueno and C Bright, "Implementing Human Rights Due Diligence through Corporate Civil Liability" (2020) 69 International & Comparative Law Quarterly 789; Robert McCorquodale and Justine Nolan, "The Effectiveness of Human Rights Due Diligence for Preventing Business Human Rights Abuses" (2021) 68 Netherlands International Law Review 455.

Downloaded from https://www.cambridge.org/core. IP address: 3.41.188.32, on 06 Nov 2026 at 13:18:20, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/err.2026.10151

with the management of risks to public values.[20] Partiti shows that human rights due diligence interacts with voluntary standards, certification, risk assessment, monitoring and remediation systems rather than replacing them.[21] Villiers similarly emphasises the complexity created by the interaction between corporate reporting, due diligence, accountability, group structures, and supply chains.[22] These studies help explain why compliance infrastructure is not incidental to risk regulation. It is the institutional form that risk regulation takes inside the firm and across the chain.

The third strand concerns contract and private ordering. Supply chain obligations often become effective through private law before they are tested through public enforcement. Sustainability clauses, supplier codes, audit rights, cooperation duties, termination rights, and model contract clauses translate public regulatory pressure into buyer-supplier relationships.[23] Contract scholarship has shown that these instruments may be understood as proactive contracting, international sales obligations, CSR clauses or transnational private governance.[24] Private auditors, certifiers, and safety experts can also become legally significant intermediaries, including through tort liability where their assurance work fails.[25]

The fourth strand concerns digitalisation and data. Due diligence is increasingly mediated by platforms, databases, satellite imagery, predictive tools, algorithmic risk scoring and remote stakeholder engagement.[26] Digital platforms may act as second-order lead firms because they structure how supply chain information is gathered, classified, and circulated.[27] More broadly, scholarship on algorithmic regulation and platform governance shows that risk classification can shift power towards technical intermediaries and corporate systems.[28] This matters because digital compliance systems intensify the very qualities that make supply chain governance attractive to regulators: visibility, standardisation, scale and repeatability.

The fifth strand concerns economic security, sovereignty and weaponised interdependence. International economic law scholarship has increasingly shown that supply access, data infrastructures, financial networks and chokepoints can become instruments of geopolitical power.[29] A related strand of Chinese international-law scholarship has examined sustainable supply chain compliance through WTO constraints, traceability and

[20] R Griffin and R Fornasari, "Risky Business? Corporate Risk Management Obligations in Sustainability Due Diligence and Digital Platform Regulation" (2025) European Journal of Risk Regulation 1 https://doi.org/10.1017/err.2025.10064.

[21] E Partiti, "The Place of Voluntary Standards in Managing Social and Environmental Risks in Global Value Chains" (2022) 13 European Journal of Risk Regulation 114.

[22] C Villiers, "New Directions in the European Union's Regulatory Framework for Corporate Reporting, Due Diligence and Accountability: The Challenge of Complexity" (2022) 13 European Journal of Risk Regulation 548.

[23] G LeBaron and A Rühmkorf, "Steering CSR Through Home State Regulation: A Comparison of the Impact of the UK Bribery Act and Modern Slavery Act on Global Supply Chain Governance" (2017) 8 Global Policy 15.

[24] J Saloranta and A Hurmerinta-Haanpää, "Proactive Contract Theory in the Context of Corporate Sustainability Due Diligence" (2022) 6 Journal of Strategic Contracting and Negotiation 221; Y M Atamer and P Wittum, "Sustainability Due Diligence in International Sales Contracts: Insights from the CISG" (2025) 30 Uniform Law Review 287; M Radchenko, "Greening the Supply Chain: CSR Clauses and Codes of Conduct in Light of the Corporate Sustainability Due Diligence Directive (CS3D) " (2025) 43 Journal of Law and Commerce 351.

[25] P Verbruggen, "Tort Liability of Private Safety Auditors in Global Value Chains" (2022) 13 European Journal of Risk Regulation 584.

[26] K H Eller and A Duval, "The 'Digital Turn' of Value Chain Due Diligence Regulation: How Technology Reconfigures Stakeholder Engagement" (2026) Global Policy 1 https://doi.org/10.1111/1758-5899.70165.

[27] J Salminen and others, "Digital Platforms as Second-Order Lead Firms: Beyond the Industrial/Digital Divide in Regulating Value Chains" (2022) 30 European Review of Private Law 1059.

[28] J Cohen, "Law for the Platform Economy" (2017) 51 UC Davis Law Review 133; Karen Yeung, "Algorithmic Regulation: A Critical Interrogation" (2018) 12 Regulation & Governance 505.

[29] M Paulsen, "The Past, Present, and Potential of Economic Security" (2025) 50 Yale Journal of International Law 22; J B Heath, "Constructing a Global Panopticon: Towards a Jurisprudence of Weaponized Interdependence" (2025) 28 Journal of International Economic Law 505.

Downloaded from https://www.cambridge.org/core. IP address: 3.41.188.32, on 06 Nov 2026 at 13:18:20, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/err.2026.10151

transparency requirements, risk allocation and the risk that compliance rules may be repurposed as instruments of economic sanctions.[30] EU market regulation itself often operates through territorial extension: it does not directly command all foreign producers, but it makes access to the EU market depend on conditions satisfied outside the EU.[31] China-focused data law scholarship likewise shows that cross-border data flows are increasingly governed through the categories of national security, data as a strategic resource, and security-assessment mechanisms.[32]

The research gap lies at the intersection of these literatures. Taken together, these literatures explain the legalisation of global value chains, the rise of mandatory due diligence, the contractualisation and digitalisation of compliance and the turn to economic security. What remains less directly theorised is the legal status of the operational infrastructure itself: how audits, contractual leverage, traceability systems, digital platforms and evidentiary flows can acquire a different legal character when sustainability compliance is performed across security-conscious legal orders.

Compliance infrastructure offers an analytical category for examining this problem. Global value chain law makes production legible; mandatory due diligence requires firms to act on that legibility; contracts, platforms and data systems operationalise those duties; and economic security law changes the legal significance of visibility itself. The concept thus captures the point at which EU sustainability risk regulation and Chinese supply chain security law meet. The question is therefore not only whether EU sustainability duties are legitimate or enforceable, but also whether the infrastructures through which those duties are performed remain legally stable across security-conscious legal orders.

III. EU sustainability law as evidentiary infrastructure

EU sustainability law is commonly described in terms of duties: to identify adverse impacts, prevent or mitigate them, bring them to an end, report on them or refrain from placing non-compliant products on the market. But these duties depend on a prior condition. They require companies to create evidence capable of linking dispersed production sites to legally relevant risks. The CSDDD and EUDR illustrate the core model, while the Forced Labour Regulation extends the same evidentiary logic into public investigation and product exclusion.

The CSDDD gives this evidentiary logic a general corporate form. Directive (EU) 2024/1760 requires in-scope companies to integrate due diligence into policies and risk management systems, identify and assess actual or potential adverse human rights and environmental impacts, prevent or mitigate potential impacts, bring actual impacts to an end or minimise their extent, establish notification and complaints mechanisms, monitor effectiveness and communicate publicly.[33] Although subsequent amendments have altered its scope and timetable, the Directive's basic technique remains infrastructural. It turns sustainability into a recurring corporate system for knowledge production, risk assessment, decision-making and review.[34]

[30] Chen and Shen, *supra*, note 15.

[31] J Scott, "Extraterritoriality and Territorial Extension in EU Law" (2014) 62 The American Journal of Comparative Law 87; J Scott, "The New EU Extraterritoriality" (2014) 51 Common Market Law Review 1343.

[32] Y Hong, "The Institutional Logic of Security Assessment of Cross-Border Data Transfers in China: Context and Progress" (2020) 1 International Cybersecurity Law Review 93; W Tan, "National Security as the Trump Card: Assessing China's Legal Regime on Cross-Border Data Transfer" (2024) 33 Information & Communications Technology Law 368.

[33] Directive (EU) 2024/1760, *supra*, note 2, Arts. 5–16.

[34] Council of the European Union, "Council Signs off Simplification of Sustainability Reporting and Due Diligence Requirements to Boost EU Competitiveness" (24 February 2026) https://www.consilium.europa.eu/en/press/press-releases/2026/02/24/council-signs-off-simplification-of-sustainability-reporting-and-due-diligence-

Downloaded from https://www.cambridge.org/core. IP address: 3.41.188.32, on 06 Nov 2026 at 13:18:20, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/err.2026.10151

The CSDDD also relies on supply chain relationships rather than solely on corporate boundaries. It expects companies to work through subsidiaries and business partners, including by seeking contractual assurances, supporting small and medium-sized enterprises where relevant, adopting prevention action plans, suspending relationships in certain circumstances, and monitoring the effectiveness of measures.[35] Recent risk regulation scholarship on the CSDDD's resilience effects is useful here because it shows how the Directive can push companies to assess vulnerabilities and redesign supplier-management practices.[36] The point is not simply that firms must comply with a new public law rule. They must produce a governance apparatus capable of translating legal risk into operational action.

This apparatus is likely to be most visible in procurement and supplier management. Buyers will need to decide what information is required at onboarding, how often supplier risk should be reassessed, what evidence is sufficient for lower-tier suppliers, which risks justify a corrective-action plan, when responsible disengagement is permissible, and how decisions should be documented. Each of these questions has a legal dimension, but each also has an infrastructural dimension. A firm can prove that it acted reasonably only if it has records showing what it knew, how it assessed risks, when it escalated concerns, and how it responded. Corporate risk management therefore becomes a form of legal memory.[37]

The EUDR is even more directly evidentiary. It prohibits relevant commodities and products from being placed or made available on the Union market or exported from the Union unless they are deforestation-free, produced in accordance with the relevant legislation of the country of production, and covered by a due diligence statement.[38] Operators must collect information, documents and data showing, among other things, product descriptions, quantities, countries of production, geolocation of plots of land, and supplier information. They must assess risk and, unless the risk is no or negligible, adopt risk mitigation procedures before market placement.[39]

Under the EUDR, lawful market access is impossible without traceability infrastructure. A product is not merely a product; it is an evidentiary bundle. Its legal status depends on the ability to link commodity, plot, producer, supplier, date, jurisdiction, deforestation status and due diligence statement. This is why the EUDR has generated intense debates about smallholders, national producer databases, interoperability, platform capacity and the distribution of compliance costs across value chains.[40] Compliance is therefore not an event at the border. It is a chain of information practices that begins upstream and travels through private and public systems.[41]

The EUDR also shows why sustainability law can become highly granular. Unlike general corporate reporting, it requires product-specific evidence of legality and deforestation-free status. That granularity can improve enforcement, but it also expands

requirements-to-boost-eu-competitiveness/ (last accessed 27 June 2026); See also Directive (EU) 2026/470 of the European Parliament and of the Council of 24 February 2026 amending Directives 2006/43/EC, 2013/34/EU, (EU) 2022/2464 and (EU) 2024/1760 as regards certain corporate sustainability reporting requirements and certain corporate sustainability due diligence requirements, OJ L, 2026/470, 26 February 2026.

[35] Directive (EU) 2024/1760, *supra*, note 2, Arts. 7–13.

[36] T Si and J B Roca, "Strengthen Supply Chain Resilience against Risks: The Impact of CSDDD on EU Companies" (2026) 17 European Journal of Risk Regulation 636.

[37] K A Bamberger and D K Mulligan, "Privacy on the Books and on the Ground" (2011) 63 Stanford Law Review 247.

[38] Regulation (EU) 2023/1115, *supra*, note 3, Art. 3.

[39] Ibid, Arts. 9–11.

[40] J Grabs, "The Construction of Compliance with the European Union Deforestation Regulation in Global Coffee Value Chains" (2025) Regulation & Governance https://doi.org/10.1111/rego.70103; H E S Nesadurai, "Challenging the EU Deforestation Regulation: Sovereignty Games as Authority Contests in Global Governance" (2026) 102 International Affairs 881.

[41] Grabs, *supra*, note 40.

Downloaded from https://www.cambridge.org/core. IP address: 3.41.188.32, on 06 Nov 2026 at 13:18:20, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/err.2026.10151

the category of information that becomes relevant to market access. Plot coordinates, production dates, supplier identities and origin documentation may be routine for one regulatory purpose and sensitive for another. The regulation therefore turns environmental legality into a data architecture. That architecture is most demanding precisely where supply chains are fragmented, informal, politically sensitive or technologically uneven.[42]

The FLR applies the same evidentiary logic through a different legal technique. From 14 December 2027, it will prohibit economic operators from placing products made with forced labour on the Union market, making them available there, or exporting them from the Union. Unlike the CSDDD's general corporate due diligence model, the Regulation operates through risk-based public investigation and product-specific enforcement. Competent authorities may request information concerning products, producers, suppliers and relevant due diligence measures. If a violation is established, the competent authority must adopt a decision prohibiting the products and ordering their withdrawal and disposal. Supply chain information thus becomes relevant not only to corporate compliance but also to case selection, investigation and market exclusion.[43]

Although the Regulation is country-neutral, its investigative architecture may have particular significance for EU–China value chains. Where suspected forced labour imposed by state authorities is at issue, information about upstream suppliers, production locations and relevant due diligence measures may become important to preliminary assessment, investigation and eventual market exclusion.[44] The Regulation therefore complements the CSDDD's relational model and the EUDR's traceability model through public investigation, while relying on much of the same compliance infrastructure.

Taken together, these instruments have two consequences. First, they change the role of the firm. The firm becomes a private evidentiary intermediary between EU public law and foreign production sites. It must translate EU legal duties, product prohibitions and investigative requests into supplier instructions, contractual warranties, audit protocols, data templates and records relevant to investigation or remediation. Second, they change the role of suppliers. Suppliers are not only producers of goods. They become producers of legally usable information. They must generate, retain and sometimes transmit evidence demanded by downstream buyers or competent authorities because market access, due diligence and product exclusion increasingly depend on that evidence.

Across this framework, three control points recur. The first is evidence production: the creation of records, certifications, maps, audits, complaints data and risk assessments. The second is supplier leverage: the contractual and commercial power through which firms seek cooperation or remediation, suspend or terminate relationships, or adjust sourcing in response to market-access and product-exclusion risks. The third is circulation: the movement of evidence through corporate groups, platforms, auditors, regulators, importers, customers and public reporting systems. These control points give EU sustainability governance operational force. They also create points of vulnerability when another legal order classifies the same practices as matters of security.

IV. Order No. 834 as a supply chain security filter

Order No. 834 should not be read as a mirror image of EU sustainability law. It does not create a general corporate due diligence regime for human rights or the environment.

[42] Ibid; Nesadurai, *supra*, note 40.

[43] Regulation (EU) 2024/3015 of the European Parliament and of the Council of 27 November 2024 on prohibiting products made with forced labour on the Union market and amending Directive (EU) 2019/1937, OJ L, 2024/3015, 12.12.2024, Arts. 3, 14, 17–20 and 39.

[44] Ibid, Arts. 8, 14(2)(a), 14(3)–(4), 17–18 and 20.

Downloaded from https://www.cambridge.org/core. IP address: 3.41.188.32, on 06 Nov 2026 at 13:18:20, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/err.2026.10151

Instead, it creates a supply chain security framework. Its stated purposes include preventing and responding to industrial and supply chain security risks, ensuring the stable and smooth operation of key industrial and supply chains, and supporting high-quality development.[45] The regime is organised around key sectors, core technologies, risk monitoring, emergency response, information systems, data, investigations and countermeasures.[46]

For the purposes of this article, the most important feature of Order No. 834 is that it treats supply chains as security infrastructures. The supply chain is not merely a market arrangement. It is a system whose interruption, manipulation or loss of controllability may become a security concern. That framing matters because it creates a legal lens through which foreign compliance conduct may be evaluated. A foreign buyer's decision to require additional information, change sourcing terms, suspend a supplier, terminate a relationship or transmit data abroad may not remain within the vocabulary of private contract or sustainability compliance. It may be assessed against the state's interest in industrial and supply chain security.

Article 13 is the first relevant filter because EU sustainability compliance often begins with information collection. Supplier questionnaires, audits, document requests, facility inspections, geolocation data and risk-screening exercises are standard compliance tools. Article 13 addresses investigations and information collection concerning industrial and supply chains within China when such activities violate Chinese law or relevant state provisions.[47] The provision does not prohibit all information gathering. Its significance is conditional: it signals that supply chain information collection becomes legally sensitive when it touches Chinese industrial and supply chain interests.

This point matters because Article 13 is not a general prohibition on due diligence, supplier audits or information requests. It is better read as a legality filter. The question is no longer only what evidence EU law requires, but whether the methods used to generate that evidence in China comply with Chinese laws, administrative regulations, departmental rules and relevant state provisions. The result is conditional visibility: information gathering may remain possible, but broad, routine or open-ended collection of compliance information becomes harder to treat as legally unproblematic.

Article 15 is the second relevant filter because EU sustainability compliance often depends on leverage. If a supplier refuses to provide evidence or take remedial action, or is classified as high-risk, the buyer may reduce orders, suspend the relationship, terminate a contract or exclude the supplier from an EU-facing supply chain. Article 15 allows security investigations when foreign organisations or individuals interrupt normal transactions, adopt discriminatory measures, or otherwise cause or threaten substantial harm to China's industrial and supply chain security.[48] The legal risk is not that every buyer decision is unlawful. The risk is that certain buyer decisions can be reclassified as discriminatory or disruptive when they operate at scale, affect strategic sectors, or appear linked to foreign regulatory pressure.

Article 15 also contains meaningful thresholds. It would be too strong to say that every supplier decision taken for EU compliance purposes becomes discriminatory disruption. Ordinary sustainability compliance should not be equated automatically with conduct threatening China's industrial and supply chain security. But it would be equally weak to treat Article 15 as irrelevant. Where exclusion, suspension, order reduction, or sourcing redesign affects strategic sectors, appears linked to foreign regulatory pressure, or

[45] State Council Order No. 834, *supra*, note 5, Arts. 1–3.
[46] Ibid, Arts. 4–12.
[47] Ibid, Art. 13.
[48] Ibid, Art. 15.

Downloaded from https://www.cambridge.org/core. IP address: 3.41.188.32, on 06 Nov 2026 at 13:18:20, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/err.2026.10151

operates through standardised risk classifications, the same decision may become open to a different legal description.

Article 16 is the third relevant filter because EU compliance is also a data flow problem. The provision should not, however, be misread as an ordinary or baseline prohibition on cross-border data transfers. Evidence does not remain where it is produced. It moves between suppliers, buyers, auditors, digital platforms, parent companies, EU importers and regulators. Article 16 comes into play after measures have been taken under the security investigation provisions and requires domestic organisations and individuals to comply with those measures. If they fail to do so, authorities may order correction and impose further restrictions, including restrictions concerning the cross-border receipt or provision of data and personal information.[49] Article 16 is therefore better understood as an escalation tool: once a supply chain security dispute has been activated, evidence circulation itself may become part of the countermeasure architecture.

This distinction matters for legal design. Describing Order No. 834 as a general data transfer ban would be inaccurate, but treating data circulation as legally neutral would be equally misleading. EU sustainability compliance depends on the repeated movement of information from suppliers to buyers, subsidiaries to parent companies, traceability platforms to auditors, and internal systems to market-access declarations, assurance files and public reports. A compliance model built on continuous evidentiary movement becomes fragile when that movement may be conditioned, restricted, or reclassified through supply chain security escalation.

Order No. 834 does not itself establish a general regime for outbound data transfers. Its data-related provisions are more specific: they link information sharing in key industrial and supply chains to data security, require enterprises and research institutions to ensure the security and controllability of core technologies, related information systems, and data, and allow further restrictions on the cross-border receipt or provision of data and personal information only after measures have been adopted under the supply chain security investigation provisions.[50] It should therefore be read in conjunction with, rather than as a substitute for, China's wider data governance framework. Separate legal instruments, including the Cybersecurity Law, the Data Security Law, and the Personal Information Protection Law, regulate network security, important data, personal information processing, and the provision of data or personal information outside China.[51] Security assessment measures and the 2024 Provisions on Promoting and Regulating Cross-Border Data Flows create a layered system in which outbound data transfers may be permitted, restricted or conditioned depending on data category, transfer volume, sensitivity and the applicable institutional pathway.[52] Order No. 834 adds a supply chain security layer to this framework: it does not replace the general data transfer rules, but it creates circumstances in which supply chain evidence circulation may be evaluated through industrial and supply chain security.

Order No. 834 also belongs to a broader family of economic-security instruments. Article 1 expressly grounds the Order in the National Security Law, the Foreign Relations Law, the Anti-Foreign Sanctions Law and the Foreign Trade Law, while adjacent regimes such as export control law regulate strategic goods, technologies, services and related

[49] Ibid, Art. 16.

[50] Ibid, Arts. 8, 12 and 16.

[51] 中华人民共和国网□安全法 [Cybersecurity Law of the People's Republic of China], as amended 28 October 2025, Art. 39; 中华人民共和国数据安全法 [Data Security Law of the People's Republic of China], Arts. 21 and 31; 中华人民共和国个人信息保护法 [Personal Information Protection Law of the People's Republic of China], Arts. 38–40.

[52] Measures for Security Assessment of Outbound Data Transfers, Arts. 4 and 8; Provisions on Promoting and Regulating Cross-Border Data Flows, Arts. 2–8 and 13; Tan, *supra*, note 32; S Guo and X Li, "Cross-Border Data Flow in China: Shifting from Restriction to Relaxation?" (2025) 56 Computer Law & Security Review 106079.

Downloaded from https://www.cambridge.org/core. IP address: 3.41.188.32, on 06 Nov 2026 at 13:18:20, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/err.2026.10151

technical data.[53] Together, these instruments contribute to a legal environment in which foreign measures, strategic goods, data, sanctions and industrial capacity may be evaluated through the lenses of sovereignty and security. This does not mean that every sustainability compliance act will be treated as hostile. It does mean that the legality of compliance cannot be assessed by reading EU instruments alone. A multinational compliance system may be designed in Brussels, but it is implemented through local contracts, local employees, local suppliers, local data and local authorities.

Order No. 834 therefore operates less as a simple prohibition than as a legal filter. It makes compliance infrastructure conditional. The same audit, questionnaire, data request, contract clause, or termination decision may pass through the filter without difficulty, require redesign, require localisation, or trigger legal concern depending on sector, actor, data, effect, and political context. This is why legal reclassification matters. The issue is not whether EU law and Chinese law always collide. It is that the legal meaning of compliance infrastructure can change when the infrastructure that enables sustainability compliance is evaluated as an object of supply chain security.

V. Three sites of legal reclassification

Building on the legal filters identified above, the following analysis focuses on three connected sites within compliance infrastructure: evidence production, supplier leverage and evidence circulation. Together, these sites trace how compliance evidence is created, used to exercise leverage and circulated through corporate and regulatory networks, while revealing the principal points of interaction with Articles 13, 15 and 16 of Order No. 834.

The first site is evidence production. EU sustainability law requires companies to produce evidence about harms, risks, origins, suppliers, plots, workers, commodities and remediation. Evidence production is normally treated as benign because it is associated with accountability. But evidence is also information about industrial organisation. In China-related supply chains, a request for supplier identity, production capacity, facility location, sourcing relationships, upstream inputs, subcontracting arrangements, or geolocation may reveal commercially and strategically sensitive information.

The problem is not that evidence production is illegitimate. The problem is that evidence production has two legal lives. In the EU legal order, it is a condition of compliance and market access. Within China's supply chain security framework, it may become an information collection practice whose legality depends on domestic law, sectoral sensitivity and the identity of the requesting actor. A single spreadsheet may therefore function both as due diligence evidence and as security-sensitive supply chain intelligence. This dual character is especially likely where evidence is collected through standardised global platforms, where foreign buyers request data directly from Chinese suppliers, or where auditors and certifiers gather information across many firms in the same sector.

The dual character of evidence also affects whose knowledge is recognised. EU sustainability compliance often privileges documentary proof, platform fields, certificates, satellite data and audit files. These forms can be useful, but they may crowd out worker testimony, community knowledge and local context. Scholarship on data and detection in international law has shown that technical systems redistribute what can be sensed and acted upon.[54] In supply chain compliance, this redistribution is legal as well as epistemic. The infrastructure determines not only what a company can know, but also what it can prove.

[53] State Council Order No. 834, *supra*, note 5, Art. 1.

[54] F Johns, "Data, Detection, and the Redistribution of the Sensible in International Law" (2017) 111 American Journal of International Law 57.

Downloaded from https://www.cambridge.org/core. IP address: 3.41.188.32, on 06 Nov 2026 at 13:18:20, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/err.2026.10151

The second site is supplier leverage. EU sustainability instruments often assume that lead firms can and should use leverage to prevent, mitigate or bring adverse impacts to an end. Contractual assurances, corrective action plans, suspension and termination are treated as tools of responsible business conduct. But leverage can also be experienced as coercion or discrimination when it is applied unevenly, follows foreign regulatory classifications, or excludes firms from market access because they cannot or will not generate the requested evidence.

This is where EU sustainability compliance may acquire security significance under Order No. 834. A European buyer may believe that it is suspending a supplier because required documentation is missing or risk mitigation is inadequate. A Chinese authority may ask whether the suspension interrupts normal transactions, imposes discriminatory measures or threatens industrial and supply chain security. The legal meaning of the buyer's act therefore depends on the frame. Sustainability law may classify the act as risk management. Supply chain security law may classify it as disruption.

The third site is evidence circulation. Compliance evidence gains value by moving. It travels from supplier to buyer, buyer to importer, importer to regulator, subsidiary to parent company, auditor to client, platform to dashboard and internal report to public-facing disclosure. This circulation is legally central to EU sustainability governance because regulators, customers and investors cannot evaluate compliance without usable evidence. But circulation also creates data-governance exposure. The more integrated and platform-based the compliance system, the more likely it is that data will cross borders, be aggregated, be reused for multiple regulatory purposes, or become accessible to foreign entities.

Evidence circulation therefore creates a double dependency. EU law depends on circulation because sustainability compliance must be demonstrable. Chinese security and data law may condition circulation because data, personal information and supply chain information are not legally neutral. This is not only a privacy issue. Some supply chain data may not be personal data at all, yet may still be sensitive because they reveal production networks, strategic capacity, bottlenecks or dependencies. The infrastructure of compliance may therefore become a map of industrial vulnerability.[55]

This point is easiest to see in relation to digital platforms. A platform may begin as a vendor tool for supplier onboarding or deforestation traceability. Over time, it may accumulate data on suppliers and production sites, together with certificates, remediation histories, delivery patterns and risk scores from multiple buyers. It may also standardise what counts as a risk and how suppliers are ranked. Scholarship on platform law shows that private infrastructures can become governance sites in their own right because they make decisions, structure participation and create internal procedures that resemble adjudication.[56] In supply chain compliance, this means that a platform may become both an accountability tool and a strategic information node. Table 1 summarises how these three sites of legal reclassification operate across EU sustainability law and China's supply chain security framework.

This reclassification analysis also clarifies why a purely conflict-of-laws framing is too narrow. The issue is not only whether two legal norms are inconsistent. Often, the norms are formally compatible at a high level: companies should respect sustainability duties and comply with domestic security and data law. The difficulty arises in the infrastructure between them. A company may be able to state both obligations, but may not be able to perform both through the same operational system. The conflict is infrastructural before it is doctrinal.

Nor should the analysis be reduced to corporate burden. The reclassification of compliance infrastructure can affect rightsholders, workers, smallholders and suppliers. If buyers respond to legal uncertainty by exiting suppliers rather than investing in lawful evidence systems, vulnerable actors may lose market access. If buyers respond by reducing

[55] Tan, *supra*, note 32; Guo and Li, *supra*, note 52.

[56] O Lobel, "The Law of the Platform" (2016) 101 Minnesota Law Review 87.

Downloaded from https://www.cambridge.org/core. IP address: 3.41.188.32, on 06 Nov 2026 at 13:18:20, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/err.2026.10151

Table 1. Three sites of legal reclassification of compliance infrastructure.

Compliance function	EU sustainability meaning	Possible security reclassification	Practical risk
Evidence production	Proof of due diligence, origin, legality or risk mitigation	Information collection affecting industrial and supply chain security	Limits on audits, questionnaires, geolocation or supplier mapping
Supplier leverage	Prevention, mitigation, remediation or responsible disengagement	Discriminatory measure, transaction interruption or supply chain disruption	Scrutiny of suspension, termination, exclusion or sourcing redesign
Evidence circulation	Demonstrability to regulators, buyers, platforms and markets	Sensitive data flow or externalisation of supply chain intelligence	Data transfer restrictions, localisation, access controls or platform redesign

transparency, sustainability harms may become less visible. If states respond by restricting information flows too broadly, accountability may weaken. The challenge is therefore not to protect firms from compliance. It is to design compliance systems that are legally defensible, rights-sensitive and security-aware.

This is why responsible disengagement must be handled carefully. EU due diligence discourse increasingly recognises that disengagement may sometimes be necessary, but that it should usually follow engagement, prevention, mitigation, remediation and attention to adverse consequences. In a security-sensitive environment, the same sequence matters for an additional reason. A documented, proportionate and remediation-oriented process is less likely to be characterised as arbitrary exclusion or discriminatory disruption than a sudden termination based on opaque risk scores. Procedure cannot remove all geopolitical risk, but it can change the legal character of a decision.[57]

VI. Implications for risk regulation and private law

The first implication is conceptual. Existing work on infrastructure as regulation, legal pluralism and supply chain infrastructures shows the value of "thinking infrastructurally": treating infrastructure as a form of ordering rather than as neutral technical support.[58] Risk regulation scholarship should therefore treat compliance infrastructure as an object of regulation in its own right. Traditional accounts focus on the regulator, the regulated firm and the risk to be managed. Supply chain sustainability law adds another layer: the infrastructure through which risk is identified, classified and acted upon. When that infrastructure becomes security-sensitive, the scope of regulation expands. Law regulates not only deforestation, forced labour, labour rights, corporate governance or market access, but also systems that make those risks visible.

The second implication concerns transnational private law. Contracts are now central sites of legal translation. A supplier clause drafted to satisfy EU due diligence requirements

[57] Deva, *supra*, note 16; A Schilling-Vacaflor and M-T Gustafsson, "Towards More Sustainable Global Supply Chains? Company Compliance with New Human Rights and Environmental Due Diligence Laws" (2024) 33 Environmental Politics 422.

[58] B Kingsbury, "Infrastructure and InfraReg: On Rousing the International Law 'Wizards of Is'" (2019) 8 Cambridge International Law Journal 171; B Turner, "Legal Pluralism in Infrastructural Designs: Alternative Supply Chains in the Moroccan Argan Oil Export" (2023) 48 Science, Technology, & Human Values 475; B Turner and M G Wiber, "Legal Pluralism and Science and Technology Studies: Exploring Sources of the Legal Pluriverse" (2023) 48 Science, Technology, & Human Values 457.

Downloaded from https://www.cambridge.org/core. IP address: 3.41.188.32, on 06 Nov 2026 at 13:18:20, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/err.2026.10151

may have effects under Chinese supply chain security law. Lawyers therefore cannot treat sustainability clauses as self-contained boilerplate. They must ask what information the clause requires, who receives it, where it is stored, how it may be reused, what happens if the supplier refuses to provide the requested information, and whether suspension or termination could be characterised as discriminatory or disruptive. Contract design must move from one-sided evidence extraction towards documented cooperation, proportionate information requirements, remediation, staged escalation and lawful data handling.[59]

The third implication concerns digital compliance platforms. Platforms can make compliance scalable, but they can also centralise sensitive supply chain information, standardise risk classifications and create opaque decision pathways. From the perspective of EU sustainability law, platform-mediated due diligence may distance companies from affected stakeholders and convert human rights or environmental questions into corporate risk scores.[60] Research on data sharing in United Kingdom modern slavery and human trafficking initiatives illustrates the broader data governance risk: systems intended to improve transparency and coordination can expose vulnerable people to further harm where sharing procedures are opaque and accountability for downstream uses is limited.[61] A related but distinct concern arises under Chinese security law, where the aggregation of supply chain information may increase its visibility, portability and strategic value. Platform governance should therefore be treated as part of legal compliance design rather than merely as the procurement of a software service.

The fourth implication concerns corporate governance. Board and senior management oversight of sustainability compliance should include a map of the compliance infrastructure's security risks and data flows. This does not mean subordinating human rights and environmental duties to security concerns; it means recognising that poorly designed infrastructure may fail under both sustainability and security law. A system that cannot lawfully collect or transfer evidence may not satisfy EU expectations. A system that collects excessive or poorly controlled information may create exposure under Chinese security and data law. Governance should therefore ask not only whether the firm is compliant, but also whether the infrastructure through which it complies is legally robust.

The fifth implication concerns regulators. EU lawmakers and enforcement authorities should be attentive to the foreign legal environments in which EU compliance systems operate. If market access rules require data that cannot lawfully be collected or transferred in certain jurisdictions without safeguards, companies may respond by de-risking, disengaging, or relying on formalistic documentation. Guidance should therefore address proportionate evidence requirements, lawful pathways for data collection and transfer, recognised alternative forms of evidence, supplier cooperation and responsible disengagement. Chinese authorities, for their part, should clarify how Order No. 834 applies to ordinary sustainability audits, traceability systems, and contractual remediation mechanisms so that security review does not unnecessarily chill legitimate accountability.

The sixth implication concerns enforcement style. The concept of "really responsive regulation" requires regulators to attend not only to the operating frameworks of regulated firms but also to the broader institutional environment of the regulatory regime.[62] Supply chain sustainability enforcement should therefore examine not only whether a firm possesses documents, but also whether its compliance infrastructure is

[59] Saloranta and Hurmerinta-Haanpää, *supra*, note 24; John F III Sherman, "Integrating Human Rights Due Diligence into Model Supply Chain Contracts" (Corporate Social Responsibility Initiative Working Paper No. 80, Harvard Kennedy School 2022) https://dash.harvard.edu/handle/1/42719205 (last accessed 30 April 2026).

[60] Griffin and Fornasari, *supra*, note 20; Eller and Duval, *supra*, note 26.

[61] J Hancock and others, "The Tensions of Data Sharing for Human Rights: A Modern Slavery Case Study" in Proceedings of the 2024 ACM Conference on Fairness, Accountability, and Transparency (Association for Computing Machinery 2024) 974.

[62] R Baldwin and J Black, "Really Responsive Regulation" (2008) 71 The Modern Law Review 59.

Downloaded from https://www.cambridge.org/core. IP address: 3.41.188.32, on 06 Nov 2026 at 13:18:20, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/err.2026.10151

capable of producing reliable and rights-sensitive knowledge through proportionate methods. Conversely, new governance scholarship warns that principles-based compliance can degenerate into internal procedures that are impressive on paper but weak in practice.[63] The relevant regulatory question is therefore not only whether a company has a policy, a platform, or a supplier code, but whether those instruments connect to genuine prevention, remediation, and lawful information governance.

The seventh implication concerns the normative evaluation of due diligence. Compliance infrastructure is necessary if sustainability obligations are to be more than symbolic, but it also redistributes power. It can shift costs upstream, privilege firms with data capacity, exclude small suppliers, empower auditors and platforms, and turn affected stakeholders into data points. The security turn adds another dimension: compliance infrastructure can redistribute strategic visibility among states, firms and platforms. Legal design must therefore evaluate infrastructure by asking what it reveals, whom it empowers, whom it burdens, and how it can be contested.

This emphasis on contestability makes participation more than a decorative feature of compliance design. It is a safeguard against both box-ticking and security overreach. If affected stakeholders, suppliers and local experts can contest risk classifications, explain missing data, propose alternative evidence and challenge disengagement decisions, the infrastructure is less likely to become a closed system of extraction and exclusion. Company law scholarship has long argued that global supply chains expose the limits of corporate law structures built around separate legal personality, shareholder value and group fragmentation.[64] Participation cannot solve those structural limits by itself, but it can make the evidentiary system less one-sided. It also helps distinguish legitimate accountability from opaque control.[65]

Taken together, these implications point towards a practical design principle: bounded interoperability. Supply chain compliance systems should be interoperable enough to satisfy EU evidence requirements, but bounded enough to respect applicable security, data governance and proportionality requirements in the jurisdictions where evidence is produced. Bounded interoperability would favour data minimisation, purpose limitation, local verification where appropriate, controlled access, audit trails, supplier participation, tiered disclosure and documented assessments of proportionality. It would also distinguish between evidence that must move across borders and evidence that can be verified locally without full extraction.[66]

Bounded interoperability is not a complete solution to geopolitical conflict or to the tension between sustainability and security. Its value instead lies in locating the compliance problem at the infrastructural level. The task is not simply to determine whether firms have duties, but to design compliance infrastructures through which those duties can be performed without turning accountability into uncontrolled information extraction or creating avoidable conflict with security law.

VII. Conclusion

Contemporary supply chain regulation increasingly operates through compliance infrastructure. Legal disputes therefore concern not only the content of duties, but also the systems through which those duties are performed. Although the CSDDD, EUDR and

[63] C L Ford, "New Governance, Compliance, and Principles-Based Securities Regulation" (2008) 45 American Business Law Journal 1.

[64] B Sjåfjell, "How Company Law Has Failed Human Rights – And What to Do about It" (2020) 5 Business and Human Rights Journal 179.

[65] Eller and Duval, *supra*, note 26.

[66] Tan, *supra*, note 32; Guo and Li, *supra*, note 52.

Downloaded from https://www.cambridge.org/core. IP address: 3.41.188.32, on 06 Nov 2026 at 13:18:20, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/err.2026.10151

FLR use different legal techniques, each depends on infrastructure that makes global production visible, evidentiary, and governable. China's Order No. 834 shows that the same infrastructure may be read through security, resilience, and controllability.

The article's core claim is one of legal reclassification: compliance infrastructure can become a security object. Evidence production, supplier leverage and evidence circulation are three connected sites at which practices necessary for sustainability governance may also attract security scrutiny. This does not make EU sustainability compliance impossible, nor does it mean that supplier audits, traceability systems, contractual remediation or data transfers are automatically unlawful. It means that their legal character can change when they operate in a supply chain security environment.

Order No. 834 sharpens this point because its most relevant provisions operate through filters and escalation rather than simple prohibition. Article 13 functions as a legality filter for certain investigations and information collection concerning industrial and supply chains in China. Article 15 creates a pathway for investigating conduct by foreign organisations or individuals where it interrupts normal transactions, involves discriminatory measures, or causes or threatens substantial harm to industrial and supply chain security. Article 16 does not impose a baseline data transfer ban, but permits further restrictions concerning data and personal information where domestic actors fail to comply with measures adopted under the investigation provisions. The legal problem is therefore not automatic doctrinal conflict, but infrastructural instability: formally compatible obligations may not always be operationally compatible within the same system.

For risk regulation and transnational private law, the broader lesson is that compliance infrastructure should be treated as an object of regulation and a form of ordering in its own right. This perspective directs attention to the organisational, contractual and digital systems through which sustainability duties become operational. Those systems determine what counts as evidence, whose knowledge becomes legible, how leverage is exercised, where information moves and whether affected actors can contest the resulting classifications. Governing sustainability risk therefore also requires attention to the architecture, participation and accountability of the systems through which compliance is performed.

For regulators and firms, this suggests a practical orientation rather than a retreat from sustainability compliance. Compliance systems should be designed for bounded interoperability: they should be sufficiently interoperable to meet EU evidence requirements, but their operation should be bounded through data minimisation, purpose limitation, controlled access, local verification where appropriate, supplier participation, tiered disclosure and documented assessments of proportionality. Such design will not eliminate geopolitical friction. It can, however, reduce the risk that sustainability compliance will be reclassified as opaque information gathering, discriminatory disruption or uncontrolled externalisation of supply chain intelligence.

Acknowledgements. The author gratefully acknowledges the institutional support of the Faculty of Law, University of Helsinki and the valuable comments of the anonymous reviewers.

Financial support. Open access funding provided by University of Helsinki.

Competing interests. The author declares none.

Cite this article: L Yuan, "When Compliance Infrastructure Becomes a Security Object: Legal Reclassification between EU Supply Chain Due Diligence and China's Order No. 834". *European Journal of Risk Regulation*. https://doi.org/10.1017/err.2026.10151

Downloaded from https://www.cambridge.org/core. IP address: 3.41.188.32, on 06 Nov 2026 at 13:18:20, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/err.2026.10151