Hennebel Avocats

PRAXIS · GUIDE

# Companies in conflict zones: a practical guide

*Hennebel Avocats Modus Operandi*

BY LUDOVIC HENNEBEL

SEPTEMBER 3, 2026

EXPOSED COMPANIES, HUMAN RIGHTS AND EXCEPTIONAL SITUATIONS

## Before you read on: if the situation is unfolding, contact the firm in confidence.

*Crisis Room - Praesidium*
A public allegation, a search of premises, a criminal allegation against an executive, a decision under pressure on whether to stay or withdraw, or a security incident at an exposed site calls for an immediate, confidential assessment. Reading the guide in full can wait. Urgent situations receive priority. *This guide is no substitute for legal advice. It guides you through the issues, but the decision is yours.*

Urgent contact

# Operational summary

A company operating in an area affected by armed conflict, serious unrest or a major crisis is no longer subject to ordinary business law alone. Depending on the legal characterisation of the facts and the jurisdictions to which the operation is connected, other bodies of law also apply: international humanitarian law, international human rights law, mandatory due diligence regimes, sanctions and export control law, and criminal law - both domestic and international. Each has its own thresholds for application, its own courts and its own timescale. The defining feature is that exposure is **cumulative**. The same event - a payment to an armed group, a delivery to a questionable intermediary, an incident involving guards at a site - can simultaneously give rise to a criminal investigation, a civil claim, duty of vigilance litigation, sanctions proceedings and a public campaign affecting the company's reputation. A response confined to one of these fronts leaves all the others open.

This guide rests on three propositions. First, **the context changes the standard**. The United Nations Guiding Principles on Business and Human Rights, endorsed by the Human Rights Council in resolution 17/4 in 2011, recognise that the risk of gross abuses is greater in conflict-affected areas (Principle 7, addressed to States, and the commentary on Principle 23). The nature of due diligence varies with the severity of the risks and the operating context (Principle 17). In its 2020 report to the General Assembly (A/75/212), the UN Working Group concluded that heightened due diligence was called for. The guide published in 2022 by the United Nations Development Programme with the Working Group set out how to carry it out. Measures sufficient in ordinary circumstances cease to suffice when the operating environment itself fosters criminal conduct. Second, **exposure now extends beyond social responsibility to binding law**. The French Duty of Vigilance

Act of 27 March 2017, the 2024 European directive on corporate sustainability due diligence - revised in 2026 and applicable from 26 July 2029 -, the 2017 European regulation on conflict minerals and criminal case law - foremost among the decisions being the judgment of the Criminal Chamber of the Court of Cassation on 7 September 2021 in Lafarge - have brought some matters that were still voluntary commitments fifteen years ago within the scope of legal obligations already in force or due to apply. Depending on the regime, these obligations carry oversight, corrective measures or penalties. The criminal courts, for their part, have applied existing offences to corporate transactions. Third, **withdrawal does not in itself afford protection**. The decision to stay, suspend operations or withdraw is itself a due diligence decision. It requires assessment, documentation and a plan for implementation in stages. A hasty exit can aggravate the impacts on people, contradict the company's earlier commitments and create fresh exposure.

The twelve steps follow a strategic order. The first three - characterising the context and identifying the applicable law, conducting heightened due diligence and mapping cumulative exposure - provide the analytical foundation. No sound decision can be taken without them. Steps four to six address the three areas in which business activities carry the greatest risk of involvement in violations: material or financial contributions that may amount to complicity, relations with public and private security forces, and the supply chain. Steps seven to nine cover the defence: responding to allegations and challenges raised through institutions, coordinating proceedings, and addressing sanctions and export controls. The final three steps concern decisions with lasting structural consequences: responsible exit, governance and documentation of decisions, and remediation and rebuilding.

This guide is intended for companies and groups facing exposure, their executives and directors, their legal, compliance and security departments, and the advisers who assist them. It sets out the order in which decisions should be taken and the authorities governing them, as the law stood on 21 November 2026, the date of the update. Matters liable to change (pending proceedings, transposition measures and reforms) are dated in the text and must be checked at the time of action. The guide is no substitute for legal advice tailored to the particular circumstances of the case.

# Executive brief: making a decision in ten minutes

**Executive decision.** Treat a conflict as a change in the legal regime, going beyond an increase in operational risk. Depending on the operations, humanitarian law, human rights law, the duty of vigilance, sanctions, export controls and criminal law apply alongside the ordinary law. The decision to stay, suspend operations or exit must be assessed, documented and reviewed. A hasty exit can aggravate impacts as much as staying

without regard to the consequences. The record of the board's deliberations becomes a central element of any future defence.

**Intended outcome.** Prevent contributions to serious violations, protect the company and its executives, coordinate the response across all fronts and ensure that each strategic decision can be defended years later.

Sequence of action

- **Assess the situation** Identify the context, applicable law, heightened due diligence requirements and cumulative exposure of entities and individuals. Deliverable: a map of the legal issues and people affected.
- **Manage points of contact** Control transactions, intermediaries, security forces, suppliers and supply chains. Deliverable: a contribution to violations prevented.
- **Defend** Respond to allegations and coordinate proceedings, sanctions, export controls and communications. Deliverable: consistent positions.
- **Decide and remedy** Assess whether to stay, suspend operations or exit, record the board's deliberations and organise remediation, return and record retention. Deliverable: a decision that stands the test of time.

Critical mistakes

- Allowing intermediaries to pay armed actors in the belief that a commercial motive offers protection. The Court of Cassation held in Lafarge on 7 September 2021 that assistance given with knowledge of the crimes being prepared or committed suffices for complicity in crimes against humanity.
- Confusing supplier certification with actual due diligence.
- Ignoring a formal notice or an allegation letter, or responding without assessing the implications for the other fronts.
- Exiting rapidly without examining the purchaser, the position of employees and the impacts of the exit.

Questions for management

- What did the company know, when did it know it and what decision followed?
- What objective criteria trigger escalation, suspension, withdrawal or remediation?
- How can internal records, public statements and duty of vigilance obligations be kept consistent?

*This summary provides initial guidance. It cannot replace analysis of the case or verification of the law applicable at the time of action. The twelve steps below set out the detail.*

# Step 01 - Characterise the context and identify the applicable law

Timing for the company: **immediately, then on an ongoing basis** · At stake: the legal characterisation of the context determines the obligations, prohibitions and courts with jurisdiction

The first decision concerns the legal characterisation of the situation, before any course of action is chosen. An international armed conflict, a non-international armed conflict, an occupation, internal disturbances below the threshold of armed conflict, a state of emergency, or a major political or public health crisis: each changes the body of law applicable to the company. The legal treatment of the same operation - extraction, production, financing, delivery or the provision of security - depends on how the context is classified. The most common error is to treat this as a question of operational risk management when the first question is which law applies.

The first aspect to assess is international humanitarian law. An armed conflict is international when it is between States, including an occupation that meets with no armed resistance. It is non-international when hostilities between a State and organised armed groups, or between such groups, meet the requisite thresholds of intensity and organisation. The existence of an armed conflict triggers the application of a body of law for which Article 3 common to the four Geneva Conventions lays down the minimum rules in non-international conflicts. Contrary to a persistent misconception, this law has direct implications for business actors. The International Committee of the Red Cross recalled in its 2006 study on business and international humanitarian law that company personnel must respect humanitarian law when their activities are closely linked to the armed conflict, that the company's property and installations can, depending on their use, lose the protection accorded to civilian objects, and that serious violations expose perpetrators - including company executives - to criminal prosecution. The 2011 United Nations Guiding Principles draw the corresponding conclusion. The commentary on Principle 12 specifies that, in situations of armed conflict, the standards that companies are expected to respect include those of international humanitarian law.

The second aspect concerns restrictive regimes: international sanctions, asset freezes, sectoral sanctions and export controls. Conflict zones are subject to a concentration of these regimes. They can turn ordinary operations - paying a supplier, delivering equipment or insuring a consignment - into transactions that are subject to conditions, prohibited or liable to give rise to criminal proceedings. Step 09 addresses how to map them. At this stage, no decision to operate in a crisis area can be taken without first checking the applicable lists and regimes. A dated record of that check must be retained.

The third aspect concerns duty of vigilance regimes. The Act of 27 March 2017 requires companies to publish and effectively implement a plan if, at the close of two consecutive financial years, they employ at least 5,000 people together with their direct or indirect French subsidiaries, or at least 10,000 together with their French and foreign subsidiaries. A controlled company exceeding these thresholds is deemed to meet the obligations if the plan drawn up and implemented by its controlling company covers its activities and those of all subsidiaries or controlled companies. The plan covers serious adverse impacts on human rights, fundamental freedoms, human health and safety, and the environment arising from the activities of the company and the companies it controls, as well as those of the subcontractors or suppliers concerned insofar as their activities relate to the established business relationship (Commercial Code, Article L. 225-102-1, I). Directive (EU) 2024/1760 of the European Parliament and of the Council - known as the CS3D or CSDDD - established an EU-wide duty of vigilance based on the UN and OECD frameworks. It was substantially revised by Directive (EU) 2026/470 of 24 February 2026, known as "Omnibus I", which entered into force on the twentieth day following its publication in the Official Journal on 26 February 2026. Its scope is assessed over two consecutive financial years. The general thresholds for EU companies are more than 5,000 employees on average and net worldwide turnover exceeding EUR 1.5 billion. For third-country companies the threshold is net turnover exceeding EUR 1.5 billion in the Union. The ultimate parent company's group can also meet these thresholds. Article 2 provides a separate route for certain franchising or licensing agreements in the Union where royalties exceed EUR 75 million and net turnover exceeds EUR 275 million, calculated worldwide for EU companies and within the Union for third-country companies. The directive no longer itself establishes the basis for civil liability, which is a matter of national law. The obligation to adopt a climate transition plan has been removed. Member States must transpose these provisions by 26 July 2028 and apply them from 26 July 2029 (for the annual statement under Article 16, from financial years beginning on 1 January 2030). Until then, the directive creates no obligations directly enforceable against companies, and the French Act of 2017 remains the applicable regime for companies within its scope. The revised directive also extends full harmonisation to most of the due diligence process - identifying and prioritising impacts, prevention and corrective action, complaints, monitoring and communication. It specifies, however, that the prohibition on reducing existing levels of protection does not prevent Member States from adapting their existing due diligence legislation, particularly its scope, to align it with the directive. The French regime may therefore change upon transposition and its terms must be checked at the time of action. The decisive point in characterising the context is that these regimes continue to apply in a crisis - indeed, their demands are greatest in conflict settings.

The fourth and final aspect is criminal law. Two bodies of rules apply to different categories of persons. International criminal law under the treaties in force - foremost among its provisions the modes of liability in Article 25 of the Rome Statute - applies for the most part only to natural persons. Executives, managers and employees face exposure in their own right, as the International Criminal Court has no jurisdiction over legal persons. The company's exposure as an entity arises under domestic criminal laws that recognise corporate liability and provide for extraterritorial jurisdiction - without prejudice to civil liability. Steps 03 and 04

address these two forms of exposure, which are distinct from those discussed above. The initial assessment must establish, jurisdiction by jurisdiction, which courts could hear the case: those of the State in which the company has its registered office, the States of its subsidiaries, the States where it operates and the States of which its executives are nationals.

## What to gather

- A map of the entities, sites, personnel and flows (financial, logistical and contractual) in the affected area.
- A documented assessment of the context: the nature of the conflict or disturbances, the armed actors present and the areas they control.
- An inventory of the applicable regimes: IHL, the duty of vigilance, sanctions, export controls and possible grounds of criminal jurisdiction.
- A timeline of decisions already taken and the grounds for them.

## What not to do

- Treating the situation simply as an operational or insurance risk without assessing its legal character.
- Making public statements before assessing the context and exposure, apart from mandatory alerts and disclosures.
- Considering only one body of law - the duty of vigilance without criminal law, or sanctions without IHL.

*Key point*

Principle 7 of the 2011 Guiding Principles is addressed to States. It calls on them to help companies operating in conflict-affected areas identify, prevent and mitigate the risks of gross abuses. Where a company is involved in gross abuses and refuses to cooperate in addressing the situation, States are encouraged to deny it access to public support and services. **Read this from the company's perspective**: a company operating in a conflict zone should expect its own State - through export credit agencies, diplomatic support and public procurement - to exert pressure and give effect to international standards. Documented cooperation is the surest means of helping the company avoid such a measure.

# Step 02 - Conduct heightened due diligence

Timing for the company: **from the initial assessment, then on an ongoing basis** · At stake: heightened due diligence is the standard against which decisions are likely to be assessed

The 2011 Guiding Principles define human rights due diligence as the ongoing process by which a company identifies its actual and potential adverse impacts, prevents and mitigates them, and accounts for how it addresses them. This is the subject of Principle 17, developed in Principles 18 to 21 (assessment, integration of findings, tracking and communication) and complemented by Principle 22 on remediation. The OECD Guidelines for Multinational Enterprises, as revised in 2023, and the OECD Due Diligence Guidance for Responsible Business Conduct, published in 2018, translate this into six practical steps: embed responsible business conduct in policies and management systems, identify and assess impacts, cease, prevent and mitigate them, track implementation, communicate and provide for remediation. This framework now provides the common basis for mandatory regimes. Directive (EU) 2024/1760 refers to it in its recitals. The French Act of 2017 follows the approach of these instruments without citing them in its operative provisions.

In a conflict-affected setting, the nature of the process changes. The 2022 guide published by UNDP with the United Nations Working Group on Business and Human Rights - on heightened human rights due diligence in conflict-affected contexts - and the Working Group's 2020 report point to three changes, which this guide summarises as follows. First, the analysis extends beyond the company's impacts on people to its interactions with the conflict itself. This requires mapping the actors involved, their sources of funding and the areas they control, and asking how the company's activities - its payments, recruitment, land purchases, security arrangements and local tax payments - fuel, mitigate or shift the dynamics of the conflict. A company may have no direct impact on human rights yet sustain the conflict that destroys them. Second, the threshold for action falls as the potential severity rises. Ordinary due diligence already gives priority, where a choice has to be made, to the most severe or irremediable impacts (Principle 24). Heightened due diligence treats the risk of association with serious violations - war crimes or crimes against humanity - as requiring immediate action even where the probability is low. Third, the time available is shorter. Conflict settings can change within weeks. An annual risk assessment will be out of date.

Principle 23 of the 2011 Guiding Principles gives this requirement its clearest practical expression - and the one with the greatest consequences. In all contexts, companies should comply with applicable laws and respect internationally recognised human rights. Wherever they operate, they should treat the risk of causing or contributing to gross human rights abuses *as a legal compliance issue*. This formulation - a soft law recommendation, with no binding force of its own - merits the attention of boards of directors. It places the risk of causing or contributing to such abuses in the realm of legal compliance - which is non-negotiable

- beyond questions of risk appetite, which a company can calibrate. French criminal case law has reached the same position by its own route (step 04).

Heightened due diligence also has a consequence for the governance of business relationships. Principle 19 of the 2011 Guiding Principles and its commentary expect a company to use its influence - its *leverage* - to prevent and mitigate adverse impacts to which it is linked through its business relationships. Where its leverage is insufficient, the company should seek to increase it. Where it still lacks leverage, it should consider ending the relationship, taking into account the adverse impacts that termination might itself cause. The commentary specifies that where the relationship is crucial to the company, the more severe the abuse, the more quickly it will need to see change before deciding whether to end the relationship. These three steps - exercise leverage, increase it, consider responsible disengagement - inform all the steps that follow. They govern relations with security forces (step 05), the supply chain (step 06) and the decision to exit (step 10).

## What to gather

- An up-to-date conflict analysis covering the actors, their funding, areas of control and the local war economy.
- A map of impacts and interactions between the company and the conflict, reviewed at short intervals with potentially affected groups or, where they cannot be consulted safely, using credible independent sources.
- An inventory of sensitive business relationships and the leverage the company can actually exercise in each.
- A dated written record of each review: findings, decisions, measures and follow-up.

## What not to do

- Rolling over the peacetime risk assessment and relabelling it “heightened”.
- Outsourcing the conflict analysis without ensuring that decision-makers take ownership of it.
- Recording risks without recording the measures taken. An identified risk with no documented response is evidence against the company.

*Key takeaway*

Heightened due diligence changes the subject of the inquiry as well as its intensity. **It examines the conflict as closely as the company**, lowers the threshold for action as severity increases, and treats the risk of causing or contributing to gross abuses as a matter of legal compliance - beyond the company's discretion to set its risk appetite.

*Spotlight*

The due diligence record serves two audiences. In real time, it guides decisions. Years later, an investigating judge, a civil court, a National Contact Point or a regulator will read it as evidence of what the company **knew, could have known and chose to do**. Write it with both readers in mind.

# Step 03 - Map the cumulative exposure of entities and executives

Timing for the company: **within the first few days** · At stake: structuring the defence requires a complete picture of all fronts - and a clear distinction between the company and its executives

In exceptional situations, exposure accumulates across several fronts. The same facts can give rise to action on at least five fronts simultaneously, each with its own rules on evidence, limitation and procedure. Mapping that cumulative exposure is a prerequisite for any strategy. It determines what can be said, written, produced and decided on each front without prejudicing the others.

**The criminal front.** This concerns the company as a legal person, in systems that recognise corporate criminal liability, and its executives as natural persons. Possible offences range from complicity in international crimes (step 04) to terrorist financing, breaches of embargoes and sanctions, corruption and money laundering. Grounds for extraterritorial jurisdiction - active and passive personality, and universal jurisdiction over international crimes in some systems - mean that proceedings may begin in a jurisdiction where the company has neither its registered office nor assets. The trial in Sweden of two former executives of a Swedish oil group for complicity in war crimes in Sudan illustrates the extraterritorial reach of prosecution. In the case of the Swiss executive residing in Switzerland, the Supreme Court expressly found a sufficient connection to Sweden. The allegations concern events between 1999 and 2003. The criminal charges are against two former executives, and the prosecution has also sought confiscation from the company of several billion Swedish kronor. The trial hearings concluded on 28 May 2026. As at 29 October 2026, the court expected to deliver judgment on 3 December. On 30 October, it postponed delivery until 11.00 on 17 February 2027. This is

the most serious front. Alongside the criminal enforcement of sanctions (step 09), it puts individuals' liberty at risk.

**The transnational civil front.** Victims of violations committed in the area of operations may bring civil claims against the company in the courts of the State where it has its registered office or in third States. The once-feared US *Alien Tort Statute* has been substantially narrowed. The US Supreme Court restricted its extraterritorial application (*Kiobel*, 2013), excluded foreign corporations from its scope (*Jesner*, 2018) and then held that allegations linking only general corporate decision-making to the United States were insufficient (*Nestlé USA*, 2021). This narrowing has changed the basis of civil exposure in the United States without extinguishing it. Claimants now invoke applicable foreign law or the law of individual US states in federal courts. On 17 October 2025, applying Swiss law, a federal jury found a French bank liable to compensate three Sudanese refugees for the bank's contribution to atrocities committed by the Sudanese regime. The judge had severed their claims for a bellwether trial. He referred to approximately ten thousand class members who had identified their claims and a possible further ten thousand. Following the hearing on 7 January 2026, the written order of 8 January rejected the challenges to the verdict and allowed an immediate appeal from the judgment concerning the three claimants. The bank appealed, and the judgment was not final as at 29 October 2026. Exposure has also extended to European courts hearing claims under domestic rules of civil liability, and to duty of vigilance regimes that provide distinct causes of action. Criminal exposure in the United States also persists. In October 2022, a French company and its Syrian subsidiary pleaded guilty there to conspiracy to provide material support to terrorist organisations in connection with payments made in Syria.

**The duty of vigilance front.** The Act of 27 March 2017 provides two enforcement mechanisms. The first is an action for an injunction, preceded by formal notice, to require the company to draw up, publish or effectively implement its vigilance plan (Commercial Code, Article L. 225-102-1, formerly Article L. 225-102-4). The second is a civil liability action for compensation for harm that compliance with the duty of vigilance would have prevented (Article L. 225-102-2, formerly Article L. 225-102-5). French duty of vigilance litigation has been centralised in the Paris Judicial Court (Code of Judicial Organisation, Article L. 211-21, introduced by Act No. 2021-1729 of 22 December 2021) and, on appeal, in Chamber 5-12 of the Paris Court of Appeal. After an initial phase concerning admissibility - on 18 June 2024 the Court of Appeal clarified the requirements for formal notice and standing - the courts have addressed the merits. On 17 June 2025, the Court of Appeal upheld an injunction requiring a group to supplement a risk map that failed to prioritise risks. On 12 March 2026, the Judicial Court held a parent company liable for breach of the duty of vigilance and ordered it to compensate for harm caused by infringements of trade union freedom at a foreign subsidiary. On 25 June 2026, it ordered an energy group to supplement its plan within six months of service of the judgment, with provisional enforcement. As at 29 October 2026 these decisions were open to appeal or under appeal. They nevertheless indicate a standard: effective identification, analysis and prioritisation of risks, appropriate measures and documented monitoring. An action under Article L. 225-102-2 is subject to

the ordinary rules of civil liability. The claimant bears the burden of proving breach of the duty of vigilance, harm and a causal link - evidential requirements that materially shape the litigation for both sides. Directive (EU) 2024/1760, as revised by Directive (EU) 2026/470, no longer creates an autonomous EU basis for civil liability. Compensation will be governed by national liability rules. Where liability is established, the directive requires full compensation without overcompensation and retains certain procedural safeguards, particularly concerning limitation periods and disclosure of evidence held by the company. French duty of vigilance litigation therefore retains its central importance for French companies.

**The sanctions and reputational fronts.** The former carries its own administrative and criminal measures (step 09). The latter lies outside the law but sets the pace for every other front. An NGO report or press investigation frequently precedes proceedings, provides material for claimants' cases and prompts enquiries from banks, insurers, sustainability rating agencies and investors. The public record of international mechanisms shows how allegations documented by civil society move from one forum to the next - from a report to a formal notice, and from formal notice to a complaint.

Finally, the assessment must distinguish carefully between the persons exposed. The parent company, the local subsidiary, group executives, local executives, expatriate employees and board members face different risks, have different interests and may in due course need different defences. Combining their interests in a single defence arrangement is a common mistake. It creates conflicts of interest that will emerge at the worst possible moment (step 08).

## What to gather

- A matrix of fronts × entities × natural persons, recording possible legal characterisations, jurisdictions, limitation periods and current status.
- An inventory of sensitive documents, recording their location, who holds them and the confidentiality rules that apply.
- A review of insurance policies (directors' and officers' liability, political risk), their terms and notification deadlines.
- An assessment of potential conflicts of interest between the company, its executives and its subsidiaries.

### What not to do

- Addressing the most visible front while neglecting the most serious. Reputational damage attracts attention, but criminal proceedings can lead to conviction.
- Responding to an NGO or a journalist with information whose implications for the other fronts have yet to be assessed.
- Allowing each department (legal, compliance, communications, security) to map its own front in isolation.

*Common mistake*
Assuming that the narrowing of the *Alien Tort Statute* has eliminated transnational civil exposure. ****The risk has diversified**: in the United States, actions under foreign law or the law of individual states have taken over from the ATS and have already resulted in a jury verdict that is under appeal. In Europe, national rules of civil liability and duty of vigilance regimes provide distinct avenues of action. Each forum offers advantages to claimants - *discovery* and jury trial in one, the duty of vigilance and actions brought by associations in the other.**

# Step 04 - Prevent criminal complicity through financing, supply or logistics

Timing for the company: before each sensitive transaction and throughout the operation · At stake: the most serious risk in this field - the risk to individuals

The principal criminal risk for a company in a conflict zone lies in the **contribution** - financing, supplies, logistics or services - it makes to those who commit international crimes, even where it does not commit those crimes itself. Three bodies of law define the scope of that risk.

The first is international criminal law. Article 25(3)(c) of the Rome Statute provides for the liability of anyone who, for the purpose of facilitating a crime within the Court's jurisdiction, assists in its commission or attempted commission, including by providing the means for its commission. Subparagraph (d) covers an intentional contribution in any other way to the commission or attempted commission of such a crime by a group acting with a common purpose. The contribution must be made with the aim of furthering the group's criminal activity or purpose where that activity or purpose involves the commission of a crime within the Court's jurisdiction, or in the knowledge of the group's intention to commit the crime. The precise threshold

for a punishable contribution - the conduct required, whether the contribution must be substantial and the requisite mental element - remains the subject of extensive debate among scholars and in international case law. The structure of the provision nevertheless establishes the decisive practical point. Providing the means to a group whose criminal policy is known gives rise to exposure even if the supplier does not share the group's aims. The personal scope of these rules must be understood precisely. The International Criminal Court has jurisdiction only over natural persons - the Rome Statute applies to executives, managers and employees. The company's exposure as an entity arises under domestic criminal laws that recognise the liability of legal persons.

The second is French criminal case law. In Lafarge, the Criminal Chamber of the Court of Cassation held in its judgment of 7 September 2021 (No. 19-87.367) that knowingly paying several million dollars to an organisation whose purpose is exclusively criminal suffices to establish complicity in crimes against humanity. It is immaterial that the payer acted to continue a commercial activity, and it need not have endorsed the design or execution of the criminal plan. The facts were extreme - the recipient was Islamic State and the amounts ran into millions. How the judgment applies to smaller payments or recipients whose activities are not exclusively criminal remains to be established. Its reach should be assessed with care, but a company cannot disregard it merely because its own circumstances appear less serious. On this point, the Court quashed the decision of the investigating chamber that had set aside the company's placement under formal investigation for complicity in crimes against humanity. The procedural context matters. The Court ruled at the judicial investigation stage on the conditions for placing the company under formal investigation. It made no finding of guilt. Two further developments have followed. In a judgment of 16 January 2024 (No. 22-83.681), the Criminal Chamber dismissed the appeal against the company's placement under formal investigation for complicity in crimes against humanity, while setting aside its placement under formal investigation for endangering the lives of others. As at 29 October 2026, the complicity allegations remained under judicial investigation. In the separate terrorist financing proceedings, the Paris Criminal Court, in a judgment of 13 April 2026, found the company and eight individuals, including former group executives, guilty of financing a terrorist enterprise through payments made in 2013 and 2014. It sentenced the former chairman and chief executive to six years' imprisonment with an order for committal to custody, and imposed on the company, in addition to the criminal fine, a customs fine for breach of international financial sanctions. The company and its co-defendants appealed, and the appeal was pending as at 29 October 2026. Two lessons are already apparent. A conviction for the related offence preceded any conviction for the international crime, and individuals were imprisoned. The underlying principle established by the 2021 judgment stands. For the Criminal Chamber, a commercial motive - continuing operations, protecting an asset or maintaining a market position - does not negate the mental element of complicity where it is established that the payer knew the recipient was preparing or committing the crimes in question.

The third body of law consists of related offences that capture the same transactions at lower thresholds: terrorist financing, breaches of embargoes and restrictive measures, and money laundering. These offences

are often easier to establish than complicity in international crimes and frequently provide the starting point for investigations. A company that confines prevention to complicity in war crimes leaves itself exposed to offences that can be proved from its accounts.

The practical requirements for prevention follow from these rules. The company must identify at-risk transactions - any payment, supply or service whose direct or indirect recipient might be an armed actor or an intermediary linked to one - and meet three requirements. It must identify the ultimate beneficiary of every transaction in the affected area, trace the route payments and deliveries actually take beyond the contractual arrangements, and establish a mandatory escalation threshold requiring any transaction involving a questionable beneficiary to be referred to group management for legal advice. Publicly documented cases show that controls fail less often because rules are absent than because local circumvention is tolerated: "facilitation" payments made by intermediaries, subcontractors acting as fronts and information filtered before it reaches head office.

## What to gather

- A map of financial, logistical and contractual flows in the area, identifying the ultimate beneficiaries.
- A dated, centralised register of incidents, unusual payment requests and contacts with armed actors.
- Legal opinions on sensitive transactions and the decisions subsequently taken.
- A written escalation procedure, with evidence that it was circulated and applied.

## What not to do

- Relying on motive ("we only wanted to keep operating"). A commercial motive does not exonerate the company when it knows what the recipient of its payments, goods or services is preparing or committing.
- Leaving local intermediaries to "manage" relations with armed actors without instructions or written reporting.
- Destroying records of decisions or allowing them to be lost. The absence of documentation counts against the company.

> *Key takeaway*
> The judgment of 7 September 2021 shifts the focus of the defence from endorsement of the criminal plan to **knowledge** - what the company knew about the recipient of its payments, goods or services, and when. Prevention requires a process for obtaining that information, assessing it and acting on it.

CASE STUDY 1

# The industrial operator that keeps a conflict-zone site running *through intermediaries*

**Configuration**

An industrial group keeps a site operating in an area that has come under the control of armed groups. Continued operations depend on local "arrangements" - payments for passage, purchases of raw materials from traders linked to the groups, and travel permits - handled by a subsidiary and intermediaries, with only partial information reaching head office. *Anonymised scenario based on publicly reported French litigation. See Court of Cassation, Criminal Chamber, 7 September 2021.*

**Risks**

Exposure of the entity and executives with knowledge of the facts to allegations of complicity in international crimes and terrorist financing. Challenges to the vigilance plan. Sanctions and embargoes depending on the area. Immediate reputational and banking exposure if the arrangements become public.

**Levers**

Immediately map transactions and ultimate beneficiaries. Stop transactions that cannot be traced. Document the decision to stay, suspend operations or exit in accordance with step 10. Establish separate defences for the company and its executives at this stage. Preserve all records.

**Critical point**

The dangerous period is when head office "does not want to know". The knowledge relevant in law can be established from internal alerts, security reports and exchanges with intermediaries - records that will be seized in the judicial investigation.

> *Contact Hennebel Avocats*
> An operation in a conflict zone, a questionable transaction or an internal alert? The firm assesses the situation in strict confidence. Urgent situations receive priority.
>
> Contact the firm

# Step 05 - Manage relations with public and private security forces

Timing for the company: before any deployment, with a review after every incident · At stake: documented practice identifies site security as a leading point of contact between companies and serious violations

The documented practice of international mechanisms identifies the protection of sites, personnel and convoys as one of the most frequent points of contact between companies and serious human rights abuses. Examples include excessive use of force by public units assigned to protect a facility, abuses by private security companies, and the provision of equipment or logistical support to forces implicated in abuses. Security arrangements must therefore be managed as a high-risk business relationship for the purposes of heightened due diligence. Treating them as a technical service delegated to the security department falls short of that standard.

For **public** security forces, the operational framework is provided by the Voluntary Principles on Security and Human Rights, adopted in 2000 at the initiative of the governments of the United States and the United Kingdom, extractive companies and non-governmental organisations. They organise the relationship around three elements. The first is a risk assessment specific to the security context - identifying potential perpetrators of violence, the record of the forces present and the State's capacity to respond. The second is structured dialogue with the authorities on the conduct of forces assigned to protect installations, including communicating concerns about past abuses. The third is a system for reporting and following up credible accounts of incidents. The legally sensitive issue is **material support**. Housing, transporting, equipping or paying public units whose record is known may constitute the kind of knowing contribution identified in step 04 as the principal risk of complicity. Any such support must be subject to prior checks and conditions, traceable and reversible. It must cease if it proves unlawful.

For **private** security providers, two instruments define the standard. The Montreux Document, adopted in 2008 at the initiative of Switzerland and the International Committee of the Red Cross, restates the relevant international legal obligations concerning private military and security companies operating during armed conflict. It identifies good practices for selection, contracting and oversight. Although addressed primarily

to States, it provides a corporate client with criteria for what a diligent contracting party should require. The International Code of Conduct for Private Security Service Providers, backed by an association and a certification mechanism, offers objective criteria for selection. Engaging a certified member subject to reporting obligations confers no immunity - but engaging a provider outside any such framework will be seen as a deliberate choice.

Contract terms give practical effect to these standards through clauses requiring compliance with international standards on the use of force, background checks on assigned personnel, a ban on unapproved subcontracting, immediate incident reporting, audit rights and a right of termination for breach. When an incident occurs - an injury, a shooting or an allegation of abuse involving site security - the company's response in the first seventy-two hours can affect years of litigation. The first priorities are assistance and protection for those affected, followed by preservation of evidence, reporting through the prescribed channels and within the applicable deadlines, support for victims, an internal investigation separate from the provider's investigation, and immediate review of the security arrangements. A security incident handled as a minor local matter can, years later, become the central piece of evidence in a liability claim.

## What to gather

- A dated and up-to-date security risk assessment meeting the standard of the Voluntary Principles.
- Private security contracts containing human rights clauses, background-check requirements and audit rights.
- A register of incidents and alerts, including action taken.
- A record of exchanges with the authorities about the conduct of public forces assigned to the site.

## What not to do

- Providing equipment, fuel, accommodation or payment, without written conditions, to units with a known record of abuse.
- Selecting a provider outside any certification framework on grounds of cost or "knowledge of the area".
- Leaving the provider to investigate incidents involving its own personnel on its own.

*Key point*

Security arrangements bring together three sources of risk examined in this guide. They may constitute a **contribution** to violations (step 04), they are a **business relationship** within the meaning of duty of vigilance regimes (step 02), and incidents arising from them are a frequent basis for transnational civil litigation (step 08). They warrant the level of oversight given to strategic decisions, beyond that normally applied to the procurement of services.

# Step 06 - Secure the supply chain and mineral sourcing

Timing for the company: **before each purchasing cycle in an affected area, with ongoing audits** · At stake: the supply chain is the route through which the conflict reaches the company

A company with neither premises nor employees in a conflict zone may nevertheless face substantial exposure there simply because it sources goods from the area. A significant share of the inputs used in the global economy passes through affected areas in mineral, agricultural commodity, textile or component value chains. Armed groups finance their operations by controlling extraction sites, trade routes and points where levies are collected. Sourcing has thus become the principal field for mandatory due diligence regimes.

The methodological reference is the OECD Due Diligence Guidance for Responsible Supply Chains of Minerals from Conflict-Affected and High-Risk Areas, now in its authoritative third edition. It provides two instruments. The first is a five-step framework: establish strong management systems, identify and assess supply chain risks, design and implement a response strategy, commission independent audits of smelters' and refiners' due diligence practices, and publish an annual report. The second - the most immediately applicable part of the Guidance - is a model policy annex distinguishing two categories of risk. The first requires immediate suspension or termination of engagement with upstream suppliers - serious abuses associated with the extraction, transport or trade of minerals, and direct or indirect support to non-State armed groups. The second calls initially for a risk management plan, which may include a temporary suspension of trade while mitigation is under way - support to public or private security forces that illegally control or tax the chain, corruption and fraudulent misrepresentation of origin, money laundering, and failure to pay taxes and royalties due. In the absence of significant and measurable improvement within six months of adopting the plan, the Guidance recommends suspending the relationship for at least three months or terminating it. Annex II retains the recommendation of immediate suspension or disengagement for the most serious risks. This graduated approach applies Principle 19 to the supply chain (step 02).

Binding law followed. Since 1 January 2021, Regulation (EU) 2017/821 has required Union importers of the tin, tantalum, tungsten and gold minerals and metals listed in Annex I whose imports reach the annual thresholds to conduct due diligence aligned with the OECD Guidance to determine whether supplies originate in conflict-affected or high-risk areas. It covers management systems, traceability and independent audits, under the supervision of national authorities. A metal importer is exempt from commissioning its own audit if it establishes that all smelters and refiners in its chain comply. Recycled metals are subject only to the obligation under Article 7(4). Stocks shown, in accordance with Article 1, to predate 1 February 2013 are excluded. For rough diamonds, the Kimberley Process provides an intergovernmental certification scheme designed to exclude from lawful trade diamonds used by rebel movements or their allies to finance armed conflict against a legitimate government. The well-documented limitations of the scheme preclude treating certification as a blanket assurance. Kimberley certification attests to a trading channel, but the buyer must still conduct its own due diligence. Finally, the chain also requires scrutiny **downstream**. Regulation (EU) 2021/821, which governs export controls on dual-use items, is a reminder that selling can be as risky as buying - the supply to actors in a conflict zone of goods, technologies or services capable of military or surveillance use is addressed in step 09.

Litigation and proceedings before non-judicial bodies - National Contact Points, grievance mechanisms and duty of vigilance proceedings - reveal three recurring vulnerabilities. The first is the gap between the contractual chain and the actual chain. Certificates of origin can be bought, traders aggregate output from different sources, and a company that relies solely on its direct supplier's declarations does not know its chain. The second is wilful blindness in the middle of the chain. Traceability breaks down at smelters, refiners and traders, and independent audits must focus there. The third is inconsistency in the records. Where a company publishes an ambitious responsible sourcing policy but cannot produce a risk map or an audit, its own public statements may become the standard against which it is judged - before a National Contact Point or a court hearing a duty of vigilance claim (step 07).

## What to gather

- A map tracing the actual chain for high-risk inputs back to the sites of origin and identifying where traceability breaks down.
- Independent audit reports on critical links (smelters, refiners and traders).
- A sourcing policy aligned with the OECD model policy annex, with contractual clauses passed down the chain.
- A register of alerts and supplier engagement plans, with deadlines and measures for disengagement.

### What not to do

- Confusing certification with due diligence. A certificate cannot replace either mapping or auditing.
- Abruptly terminating a supplier relationship at the first alert when graduated engagement is possible - reflexive disengagement shifts the problem without addressing it and may aggravate the impacts.
- Publishing commitments that internal records cannot substantiate.

*Spotlight*

The OECD Minerals Guidance underwent a quiet but decisive change. Conceived as a voluntary framework, it became **a standard incorporated by reference into binding law** - Regulation (EU) 2017/821 bases its obligations on it. The 2018 general Guidance is following the same course under Directive (EU) 2024/1760. Today's soft law shapes tomorrow's litigation.

## Step 07 - Respond to allegations or challenges and manage communications

Timing for the company: **within the time allowed - often short** · At stake: every written response becomes part of the record on every other front

A challenge to a company facing exposure rarely begins in court. It starts with an NGO report, a press investigation, an allegation letter from a United Nations special procedure, a specific instance submitted to an OECD National Contact Point, or a formal notice under the duty of vigilance. Each has its own rules. In every case, the company's response - or its silence - will form part of the record in subsequent proceedings.

**The OECD National Contact Point.** Each State adhering to the OECD Guidelines maintains a National Contact Point responsible for examining "specific instances" raised concerning companies. This is a non-judicial mechanism. It conducts an initial assessment of admissibility, offers good offices and mediation, and then publishes a final statement that may find that a company has failed to observe the Guidelines. This is precisely where its influence lies. The final statement is public, is cited by the press, investors and claimants in court, and records any refusal to participate. The 2023 edition of the Guidelines strengthened expectations concerning transparency and follow-up. A company facing a specific instance must decide whether to participate voluntarily, taking a position consistent with its submissions on other fronts, or to abstain and face a final statement prepared without its input. That choice requires preparation.

**United Nations special procedures.** The Human Rights Council's special rapporteurs and working groups - foremost among them the Working Group on Business and Human Rights - send allegation letters inviting companies to respond to documented allegations. According to the report on the activities of the special procedures in 2024, submitted to the Human Rights Council in 2025 (A/HRC/58/70), communications are made public sixty days after they are sent, in a database that also publishes responses received. If a response does not arrive within the time specified in the letter, the communication may stand alone on the public record when published. The practice should be checked at the time of response. A factual, documented response that avoids blanket denials can place the company's position on record. Silence leaves the opposing account as the only one in the public record.

**Formal notice under the duty of vigilance.** Under French law, an action for an injunction must be preceded by formal notice requiring compliance with the obligations concerning the vigilance plan. Proceedings may be brought only after three months have elapsed from the notice. If the company has not met its obligations within that period, the court may, on the application of any person with standing, order compliance, where appropriate subject to a periodic penalty payment, including in interim proceedings (Commercial Code, Article L. 225-102-1, II, formerly Article L. 225-102-4). On 18 June 2024 the Paris Court of Appeal held that formal notice is a mandatory prerequisite for which service of the originating summons cannot substitute. The notice must clearly set out the alleged breaches and make a firm demand of the company. There must be a sufficient connection between the complaints in the notice and those in the summons, although a fresh notice is not required each time the plan is revised. The first step for the defence is therefore to examine the validity of the notice - the company addressed and the specificity of the complaints - while reviewing the plan. Standing is assessed subsequently for each claimant, who may differ from the signatories. The three-month period provides time to revise the plan, document the measures actually taken, enter into dialogue with those who issued the notice - or prepare the defence to litigation. The worst use of that time is to let it pass in silence.

**Crisis communications.** These must be treated as acts with legal consequences. Any public statement - a press release, an interview, a response to an NGO or a non-financial disclosure - may be produced in criminal, civil and duty of vigilance proceedings in France or abroad. Opposing parties exploit implicit admissions, unfulfilled promises and contradictions across publications. At a minimum, statements require legal clearance, apart from legally required alerts and disclosures. There should be one spokesperson for each front, consistency checks across public statements, submissions in litigation and compliance documents, and a copy of every statement in the central file. Silence also has consequences - it sustains the opposing account and prompts questions from banks and investors. The narrow course between silence and a risky statement must be worked out for each front.

## What to gather

- The exact text of the allegation or formal notice, who issued it, its deadlines and the mechanism through which it was made.
- A documented account of the due diligence measures on which the company can rely (steps 02, 05 and 06).
- A table for checking consistency across positions already taken on each front, earlier publications and public commitments.
- An internal timeline of the alleged facts, prepared before any response.

## What not to do

- Issuing an unsupported blanket denial - it commits the company to an untenable position.
- Ignoring an allegation letter or formal notice in the hope that no action will follow.
- Issuing crisis communications without legal clearance or promising measures the company will not implement.

*Common mistake*
Treating the OECD NCP process as minor because the NCP cannot impose a penalty. **Its final statement remains on the public record**: civil claimants, NGOs and investors cite it, and any refusal to participate is recorded. In this field, the authority of a public finding often carries more weight than the absence of a formal sanction.

CASE STUDY 2

# A group served with a duty of vigilance notice *over its subsidiary's activities*

**Configuration**

A coalition of NGOs and local authorities serves formal notice on a French group under the Act of 27 March 2017. It alleges that the group's vigilance plan fails to address risks arising from a subsidiary's operations in an area of serious unrest - land grabbing, abuses against human rights defenders and site security. *Anonymised scenario based on publicly reported French duty of vigilance litigation. See Act No. 2017-399, Commercial Code, Article L. 225-102-1 (formerly Article L. 225-102-4).*

**Risks**

An action for an injunction after the three-month period expires. A liability claim under Article L. 225-102-2 (formerly Article L. 225-102-5) if harm has occurred. Publicity surrounding the notice and repercussions on other fronts (NCP, press, investors).

**Levers**

On receipt, check the validity of the formal notice, the specificity of the complaints and whether the demand made of the company is sufficiently firm. At the same time, use the three-month period to conduct an expedited audit of the plan and its actual implementation in the area concerned, document corrective measures and enter into structured dialogue with those who issued the notice. In parallel, prepare the defence to litigation and the table for checking consistency across positions. If a summons is served, check the connection between its complaints and those in the formal notice, then the standing of each claimant, who may differ from the signatories. Apply the criteria established by the Paris Court of Appeal: for local authorities, assess the local public interest in relation to the alleged risk and, for associations, the connection with their statutory objects.

**Critical point**

The dispute will turn less on the existence of the plan than on its **effective implementation**. Written measures unsupported by evidence of implementation count against a group that has itself defined the standard by which it will be judged.

# Step 08 - Manage proceedings and coordinate the defence across fronts

Timing for the company: from the first procedural step, with ongoing coordination · At stake: what is said on one front can defeat the defence on another

When an allegation leads to proceedings - the opening of a criminal investigation, service of a civil claim or an action for an injunction under the duty of vigilance - the company enters a phase in which **coordination** matters more than the conduct of any single proceeding. Proceedings inform one another. Documents produced in civil litigation provide evidence in criminal proceedings, public statements inform the opposing party's submissions, and findings by non-judicial mechanisms make their way into court files. Before taking any step on one front, assess its effect on all the others.

**The criminal front** has the longest timescale and the gravest consequences. Investigations into conduct in conflict zones last for years. In several European States, units specialising in international crimes have developed substantial cross-border investigative capacity. The first requirement is to preserve all documents immediately upon learning of the investigation - destroying or removing material capable of assisting the search for evidence may constitute a separate offence where the purpose is to obstruct the ascertainment of the truth (Criminal Code, Article 434-4), and in strategic terms it amounts in any event to an admission. Interviews also require care. No executive or employee should be interviewed without first being informed of their rights and, where their circumstances warrant it, assisted by their own lawyer. Witness preparation must preserve the witness's freedom to give their own account. Discussing the facts with a witness does not in itself constitute witness tampering. Article 434-15 of the Criminal Code penalises, among other things, pressure, promises or manoeuvres intended to induce a false statement or a failure to testify, even if unsuccessful. Multiple jurisdictions also require attention - several States may investigate the same facts, with documents circulating under rules on cooperation and mutual legal assistance. Several procedural deadlines operate as time bars. Under Article 173-1 of the Code of Criminal Procedure, in the version applicable to applications made on or after 23 October 2026, a person placed under formal investigation - whether a company or an executive - must, on pain of inadmissibility, raise any grounds for the nullity of acts preceding questioning at the first appearance, or of that questioning itself, within four months of delivery of the first copy of the documents in the file, provided that the person requested it within seven clear days of being placed under formal investigation. In the absence of such a request, the period runs from notification of placement under formal investigation. The bar does not apply to grounds the person could not have known. For subsequent acts, a four-month period runs from each questioning or notification of each act. After notice of completion of the judicial investigation has been sent, the parties have one month if the person under formal investigation is in custody, and three months in other cases, calculated from dispatch of the notice, to make requests and

lodge applications, including applications for nullity. After that period, they are inadmissible. This window does not reopen either the four-month period under Article 173-1 for raising nullities or the six-month period under Article 82-3 for invoking a limitation period that had already expired by the time of placement under formal investigation or the first interview as a witness with assisted status. The latter period runs from the procedural act concerned. Once the one- or three-month period expires, a further ten days are available for supplementary observations in light of the submissions communicated (Article 175). Act No. 2026-651 of 23 July 2026, which amended Article 173-1, also requires a party, for applications governed by the reform applicable from 23 October 2026, to restate all its grounds of nullity in its final written submissions to the investigating chamber. Omitted grounds are deemed abandoned even if raised in an earlier submission (Article 198). Two filing deadlines must also be distinguished. Before the investigating chamber, the ordinary deadline for written submissions expires three days before the hearing, subject to grounds of nullity that could not have been known. In matters of pre-trial detention, submissions may be filed with the registry up to and including the day of the hearing. Check also the requirements for communication and receipt specific to the method of transmission (Article 198). Where the chamber is seised under Article 173 or 221-3, submit all ascertainable grounds of nullity relating to the proceedings transmitted to it, failing which the right to raise them is lost (Article 174). Before the criminal trial court, raise procedural objections before any defence on the merits. Except in cases governed by Articles 395 to 397, file written submissions with the registry three days before the hearing, on pain of inadmissibility, unless the ground of nullity could not have been known or the summons or notice to appear was issued less than twenty days before the hearing. Following referral by an investigating court, also check which nullities can no longer be raised and the exceptions under Article 385. These article numbers were in force on 29 October 2026. A recodification takes effect on 1 January 2029. The Praxis guide to transnational investigations and inquiries sets out these steps in detail. For conflict zones, the essential point is that evidence of the events is in inaccessible territory. This gives particular weight to the company's internal records - material that both prosecution and defence can use and that must be tested against witness accounts and third-party documents.

**The civil and duty of vigilance fronts** turn largely on evidence and procedure: international jurisdiction, applicable law, access to internal documents and the admissibility of collective actions or claims by associations. The narrowing of the ATS (step 03) has not closed the US courts. It has opened a second arena in Europe, where actions under domestic liability rules and duty of vigilance regimes are increasing. A defendant company should expect its compliance documents - vigilance plans, risk maps, audits and codes of conduct - to be central to the dispute. What the company wrote about its own risks establishes which risks it identified and bears on the assessment of what it should have done. This is why due diligence records must be drafted from the outset with both audiences in mind (step 02).

**Coordination across fronts** requires a defined structure. A single coordinating counsel should maintain a complete record of proceedings, positions, documents produced and deadlines. Separate defence teams are needed where interests diverge, particularly between the company and current or former executives whose

defences may become incompatible as the investigation proceeds. Common rules must govern document handling - who produces what, where and under which rules of confidentiality - in compliance with the French blocking statute (Act No. 68-678 of 26 July 1968). Subject to applicable international treaties or agreements and the laws and regulations in force, the statute makes it a criminal offence to request, seek or disclose economic, commercial, industrial, financial or technical documents or information intended to constitute evidence in or for foreign judicial or administrative proceedings. Before producing anything abroad, assess the available channels of mutual legal assistance and the applicable conventions. Under Decree No. 2022-207 of 18 February 2022, any request covered by the statute must be reported without delay upon receipt to the minister responsible for the economy through the Strategic Information and Economic Security Service. All public statements must pass through a single clearance point (step 07). The confidentiality rules for communications with lawyers vary by jurisdiction, provide uneven coverage for in-house counsel and are subject to exceptions. Under French law, in searches and seizures governed by Articles 56-1 and 56-1-1 of the same Code, legal professional privilege for legal advice cannot be invoked against investigative measures concerning the offences exhaustively listed in Articles 1741 and 1743 of the General Tax Code and Articles 421-2-2, 433-1, 433-2 and 435-1 to 435-10 of the Criminal Code, or the laundering of the proceeds of those offences, where the legal opinions, correspondence or documents establish that they were used to commit or facilitate those offences (Code of Criminal Procedure, Article 56-1-2). For advice given by in-house counsel, Decree No. 2026-1054 of 17 November 2026 sets 1 January 2027 as the date on which the protection established by Act No. 2026-122 of 23 February 2026 enters into force. It cannot be invoked before that date. Protection depends, among other things, on the author's qualifications and training, the recipients, and how the advice is marked and filed. It cannot be invoked in criminal or tax matters. Identifying the privileges applicable to each sensitive document is a substantial task in its own right and should be completed before requests for production arrive.

> *Key point*
>
> In conflict-zone cases, evidence from the ground is often beyond reach - sites are inaccessible, witnesses dispersed and States uncooperative. The case then turns on **internal records**: emails, security reports, alerts and minutes. A company that arranges for their preservation retains control over how it uses them. A company that allows them to deteriorate is left to contend with the use others make of them.

> **Before the board takes a high-risk decision, the company responds to an allegation or new proceedings begin.**
>
> *When to contact the firm*
>
> As soon as there is an allegation, a formal notice, an investigation or a criminal allegation against an executive - and ideally earlier, when deciding whether to operate, stay or exit. The firm can act as lead counsel, as co-counsel with criminal lawyers and corporate law firms, or as a strategic adviser to legal departments. The initial discussion is confidential and entails no commitment. Urgent situations receive priority.
>
> Have your situation assessed

## Step 09 - Manage sanctions and export controls in a conflict zone

Timing for the company: **before each transaction, with continuous monitoring** · At stake: this is the fastest-changing regime in the field and one in which criminal exposure can arise most quickly

Conflict zones are subject to a concentration of restrictive measures: individual sanctions - asset freezes and prohibitions on making funds or resources available to designated persons and entities -, sectoral sanctions affecting entire sectors of an economy, arms embargoes, financial restrictions and, alongside them, export controls. For a company operating in or dealing with an affected area, this field presents three particular dangers. The rules change abruptly as successive sanctions packages are adopted. They are fragmented across regimes - United Nations, European Union, US regimes with de facto extraterritorial reach, and national regimes - with different lists and thresholds. Breaches can rapidly give rise to criminal liability. The Union is harmonising this aspect. Directive (EU) 2024/1226 requires Member States to criminalise the violation and circumvention of Union restrictive measures and to provide for the liability of legal persons. The transposition deadline was 20 May 2025. Implementation in each relevant State must be checked at the time of the transaction.

Three tasks account for most of the operational risk. The first is **in-depth screening**. Designation lists do not capture ownership structures, and an unlisted counterparty may be owned or controlled by a designated entity - sanctions regimes address ownership and control beyond the names on the lists, under rules specific to each regime. In conflict zones, where opaque ownership is the norm and armed actors operate

through front companies, name screening alone creates an illusion of compliance. The company must trace ownership to the ultimate beneficial owners. The second is **export control**. Regulation (EU) 2021/821 requires authorisation for the export of listed dual-use items. Its catch-all provisions allow authorisation to be required for unlisted items because of their destination or end user - particularly where they are intended for military use in an embargoed country. The regulation also specifically governs cyber-surveillance items. Supplying communications equipment, civilian drones, location software or surveillance technologies to a conflict zone can therefore trigger authorisation requirements. Failure to obtain authorisation attracts penalties under the regime established by each Member State, including criminal penalties where applicable. The third is **payment management**. Formal banking channels contract in affected areas. The operational temptation to switch to cash, intermediaries or informal channels is precisely what can turn a compliance problem into a criminal case - bringing it within the risk discussed in step 04.

Conflict zones also create dilemmas that mechanical compliance checks cannot resolve: continuing to pay local employees in territory that has come under the control of a designated entity, transporting humanitarian aid through checkpoints where levies are collected, or disposing of a local asset when the plausible purchasers are linked to designated persons. These situations require a documented, case-specific legal assessment before the transaction - including available derogations and authorisations, humanitarian exemptions and wind-down licences. The Praxis guide to international sanctions addresses challenges to designation and delisting. The issue for the operator here is how to avoid both complete paralysis - which has its own human and contractual costs - and carrying on "as before" under cover of local arrangements.

## What to gather

- Documented screening of counterparties in the area, including beneficial owners and ownership structures.
- Export classifications for the goods and technologies supplied, with the authorisations required and obtained.
- A map of the payment channels actually used and their vulnerabilities.
- Legal assessments of sensitive transactions (payroll, humanitarian activities and disposals) completed before execution.

### What not to do

- Screening names without tracing ownership and control.
- Switching to cash or intermediaries when banking channels close - the shortest route to criminal exposure.
- Assuming a humanitarian exemption applies without checking each regime.

CASE STUDY 3

## A bank with a client *subject to sectoral sanctions*

**Configuration**

A European bank has an industrial client whose business, following a new package of measures, now falls within a sector targeted by conflict-related sectoral sanctions. The client is not individually designated. Its customers and part of its ownership chain are in the affected area. *Anonymised scenario based on publicly documented practice under European Union sectoral sanctions regimes.*

**Risks**

Breach of sectoral measures by executing transactions that are now prohibited. Indirect provision of funds to entities owned or controlled by designated persons. Criminal exposure for the bank's executives. Conversely, contractual liability for an unjustified withdrawal of banking facilities.

**Levers**

Assess the sectoral measures transaction by transaction and trace the client's chain of ownership and control. Suspend prohibited transactions and, where appropriate, obtain the required authorisation before execution. For facilities that remain lawful, assess separately whether to maintain them or pursue a reasoned and documented exit, taking account of the contract, notice requirements and, where applicable, the Blocking Regulation.

Critical point

Overcompliance - terminating all relationships without assessment beyond what the regime requires - has consequences. It may give rise to contractual litigation and transfer the risk to the client without reducing it. The lists themselves do not define the outer limit of risk. Anti-circumvention provisions in EU sanctions regulations, anti-money laundering due diligence obligations and exposure to foreign regimes with extraterritorial reach may justify an exit extending beyond the prohibited transactions alone. A qualification applies to the foreign regimes listed in the Annex to Blocking Regulation (EC) No. 2271/96, which prohibits EU operators from complying with them without Commission authorisation. According to the Court of Justice (21 December 2021, Bank Melli Iran, C-124/20), an operator need not state reasons for termination. However, where the evidence indicates that the purpose was to comply with those regimes, the operator must establish the contrary. The termination may be annulled provided that annulment does not have disproportionate effects on the operator in light of the economic losses it would face. An application to the Commission for authorisation preserves the operator's position but does not suspend the prohibition pending a decision. If the listed laws or actions based on them affect the operator's economic or financial interests, even indirectly, Article 3 also requires it to inform the Commission within thirty days of becoming aware of the effect. For a legal person, the obligation rests on its directors, managers and other officers. A decision is defensible when the reasons are recorded, the action is proportionate and documented, and the applicable notice periods are observed.

# Step 10 - Decide whether to stay, suspend operations or withdraw: responsible exit

Timing for the company: **assess the decision away from immediate pressure and review it whenever the context changes materially** · At stake: staying and leaving both carry risks - only a properly assessed decision can be defended

Most companies operating in affected areas reach a point when the question changes from "how do we operate?" to "should we stay?". No other decision attracts closer scrutiny. Years later, courts, international mechanisms, investors and the public will assess it in light of what happened afterwards. The only defensible decision is a **properly assessed** one - taken in accordance with heightened due diligence, on the basis of a documented analysis of the impacts of each option.

The analytical framework follows from the 2011 Guiding Principles and the 2022 UNDP guide. The first lesson is that exit is not inherently the responsible default. A hasty withdrawal can aggravate impacts - local employees may be abandoned and lose their protections, assets may be sold to purchasers linked to parties to the conflict who will put them to more harmful use, essential services to communities may be interrupted, and the last actor exercising a moderating influence may disappear. The commentary on Principle 19 specifically recommends considering the adverse impacts of ending a relationship when deciding whether to terminate it. The second lesson is that staying is defensible only if it is **conditional** - with heightened measures, explicit triggers for review (a change in territorial control, the designation of a counterparty, a serious incident) and a preserved capacity to exit. Staying by default, without documented review, is the least defensible position. The third lesson is that suspension - a temporary halt while safeguarding assets and personnel - is an often overlooked intermediate option. It has risks of its own (requisition of idle assets, loss of control over facilities), but it allows the emergency decision to be taken separately from the final one.

Once decided upon, an exit is itself a high-risk legal transaction. Its lawfulness must be checked on every front: sanctions - disposing of assets in an affected area may transfer resources to designated persons or require authorisations -, local law - which may penalise cessation of operations or provide for expropriation of those leaving -, contracts - exit clauses, guarantees given and potential arbitrations (on investment protection and arbitration in conflict zones, see the Praxis guide to investments in conflict situations) - and the duty of vigilance - exit does not end obligations concerning impacts already caused. The prospective purchaser must be audited as rigorously as a high-risk supplier. Selling a site to an operator that can be expected to remove protections effectively transfers future violations to another party while leaving a record of having created the conditions for them. Finally, the sequence of withdrawal must be consistent. A company that has publicly justified staying by reference to its protective role cannot withdraw overnight without exposing the contradiction - it must be able to explain the exit as the application of its announced review criteria rather than a flight from the situation.

## What to gather

- A documented comparison of the three options - staying subject to conditions, suspension and exit - and their respective impacts on people.
- Explicit triggers for review and a review timetable.
- An audit of the prospective purchaser or successor operator and an assessment of the lawfulness of the transfer (sanctions, local law and contracts).
- A plan for addressing residual obligations towards employees and communities and continuing remediation.

### What not to do

- Exiting under media pressure without assessing the impacts of the exit itself.
- Selling to a purchaser that has not been audited in order to close the matter.
- Staying by default without review triggers or a record of review.

*Key takeaway*

Every court, mechanism and counterparty will look beyond "did you stay or leave?" to ask "**how did you decide?**". A decision to stay that was properly assessed, made subject to conditions and reviewed can be defended. A hasty, unexamined exit can count against the company as surely as staying without regard to the consequences.

CASE STUDY 4

## The hasty exit *that increases exposure*

**Configuration**

Under pressure from a media campaign after a region descends into conflict, a group publicly announces its "immediate and complete" withdrawal. The sale of its local assets, concluded within weeks with the only available purchaser, is accompanied by dismissal of local staff and abandonment of the community grievance mechanism. The purchaser proves to have links to a party to the conflict. *Anonymised scenario drawing on the lessons of the 2022 UNDP guide on heightened due diligence and responsible exit.*

**Risks**

A duty of vigilance challenge concerning the impacts of the exit itself. Possible breach of restrictive measures depending on the purchaser's links. A contradiction with the earlier reasons for staying that can be used against the group. Possible loss of leverage over remediation of past impacts, to be assessed against the rights retained, the group's own resources and any arrangements still open to negotiation with the successor operator.

| | |
|---|---|
| Levers | Regain control through a retrospective assessment. Audit the sale and the rights retained, identify possible corrective measures (enforcement of monitoring clauses or an amendment negotiated with the purchaser, funding for the grievance mechanism, support for former employees), document the actual sequence of decisions and prepare a table for checking consistency across the fronts that remain open. |
| Critical point | The public announcement of an "immediate and complete" withdrawal set a standard. Every discrepancy between the announcement and the actual exit becomes evidence available to the opposing party. Draft an exit announcement with the same care as a submission in litigation. |

# Step 11 - Governance: document the decision and the due diligence

Timing for the company: **before each high-risk decision, under standing governance arrangements** · At stake: the record of the board's deliberations is the directors' first line of defence

All the preceding steps lead to the boardroom. It is there that high-risk decisions are taken - or left untaken - on whether to operate, stay, suspend operations, exit, respond or settle. The deliberative process itself will come under scrutiny. A decision open to question on its merits is easier to defend if it was rigorously assessed. A substantively defensible decision taken without documented analysis exposes the company and, where fault can be attributed to them personally, its directors and executives - on grounds of mismanagement and, in the most serious circumstances, under criminal law. Knowledge of the risks on the part of the governing bodies is precisely what the offences discussed in step 04 put in issue. A documented deliberation does not, however, authorise a prohibited transaction.

The minimum governance arrangements comprise four elements. **A procedure for referral to the board**: exceptional situations must be brought before the board of directors under predefined criteria - independently of media pressure - with a decision file containing the legal characterisation (step 01), the status of due diligence (step 02) and the assessment of exposure (step 03). **Prior legal advice**: every high-risk decision should be preceded by a written legal analysis covering the relevant fronts and the options rejected. Consider confidentiality from the moment the advice is commissioned - the status of legal opinions varies between

jurisdictions and proceedings, and an opinion drafted without care can become evidence for the opposing party. **A record of deliberations**: agendas, papers provided to the board and minutes recording the questions asked, the options considered, the reasons for the decision and any conditions attached. Terse minutes - "the board approves" - forfeit the first line of defence. **Follow-up**: a conditional decision whose conditions go unmonitored becomes, in retrospect, an unconditional one. The board must arrange to monitor the review triggers it has set (step 10).

These arrangements must work alongside disclosure obligations. The vigilance plan and its implementation report, the sustainability information required under European law, and the company's public commitments together form a body of statements whose consistency with actual operations is itself an issue in litigation. Discrepancies between statements and practice support duty of vigilance claims, reports to regulators and allegations of misleading practices. The drafting rule is consistent: publish only what internal records can substantiate and have litigation counsel review every disclosure that creates exposure - they will have to defend it.

## What to gather

- Written criteria for referring exceptional situations to the board.
- Legal opinions obtained before high-risk decisions, with the applicable confidentiality rules identified.
- Reasoned minutes recording the options considered, grounds for the decision, conditions and review triggers.
- A table checking disclosures (vigilance, sustainability and commitments) against the documented facts.

## What not to do

- Taking a board decision without supporting papers or written legal analysis.
- Drafting minutes so terse that they leave no evidence of the deliberations.
- Publishing commitments that the company cannot substantiate internally.

*Spotlight*

The difficulty with documentation is that it works both ways. It protects the company by proving due diligence and exposes it by proving knowledge. Keeping fewer records is no solution - the absence of a record counts against the company. Keep records **with discipline**: accurate facts, signed analyses, reasoned decisions and a record of follow-up.

# Step 12 - Rebuild: return, remediation and reparations

Timing for the company: **remedy as soon as harm is identified, possible return after stabilisation, over a period of several years** · At stake: remediation determines the prospects for restoring the company's legal standing, banking relationships and reputation

The crisis comes to an end - the conflict becomes frozen, the area stabilises, and proceedings run their course or are resolved. The phase that follows has received the least attention in the literature, yet is the most consequential for the company's future: rebuilding. It involves three tasks.

**Remediation.** The third pillar of the 2011 Guiding Principles - access to remedy - extends beyond States. Under Principle 22, a company that has caused or contributed to an adverse impact should provide for or cooperate in its remediation through legitimate processes - an expectation that duty of vigilance regimes are increasingly making enforceable. Operational-level grievance mechanisms - accessible, predictable, equitable and transparent - are the usual means. The OECD guidance treats them as part of due diligence itself. After a crisis, remediation takes various forms: compensation, site rehabilitation, support for communities and participation in collective reparation mechanisms. Its design requires care in light of possible litigation. Remedial measures may be construed as admissions, so they must be coordinated with pending proceedings, insurers and defence positions. That need for care cannot serve as a pretext for inaction. A complete absence of remediation sustains the remaining disputes and prevents rehabilitation.

**Resolving outstanding matters.** Rebuilding requires a methodical effort to resolve what can be resolved: civil settlements, negotiated outcomes in proceedings where the system permits them, closure of specific instances before NCPs with follow-up on commitments made, and the gradual lifting of banking and insurance restrictions. The closure of each matter must be documented and the record placed in the central file. Banks, insurers and business partners will require evidence that past exposures have been extinguished or provided for. The quality of that evidence determines how quickly financial standing can be restored.

**Return.** Returning to an area the company left - or reinvesting in an area that has stabilised - amounts to a fresh entry into a changed environment. It calls for full heightened due diligence (step 02), an audit of pre-crisis partners - some of whom will have changed in character during the conflict - and incorporation of the documented lessons of the crisis. What the company has learned about its vulnerabilities forms part of what a court will later consider it knew. A company that returns with its pre-crisis controls risks repeating the same sequence, with an aggravating circumstance: it has happened before.

*Key takeaway*

Remediation is more than a reputational choice. It is the **third component of the standard** - prevent, mitigate, remedy - and without it the company remains exposed on fronts that the end of the crisis should have closed. Remediation should be designed in coordination with litigation counsel.

*Caution*

The crisis records - the central file, matrices, opinions and minutes - must outlast the crisis. Proceedings concerning acts committed in conflict zones sometimes begin years after the events, as political circumstances and access to evidence change - under French law, prosecution of crimes against humanity is subject to no limitation period, while the limitation period for war crimes is thirty full years from the date of the offence (Code of Criminal Procedure, Article 7). Organised long-term retention of the file, in compliance with data protection rules, is part of the defence and goes beyond routine archiving.

CRITICAL OVERVIEW

## Mistakes that *compromise the defence*

01 **Reacting before characterising the situation.** Armed conflict, unrest, occupation or crisis: each characterisation changes the applicable law, prohibitions and courts with jurisdiction. A decision or statement made before the assessment commits the company to a framework it did not choose.

02 **Addressing a single front.** Exposure is cumulative. A response drafted for an NGO may overlook the investigating judge, while one drafted for the judge may overlook the NCP. Concessions made on other fronts strengthen the case on every neglected one.

03 **Carrying over peacetime due diligence.** In a conflict-affected context, the standard is heightened due diligence: conflict analysis, a lower threshold for action on serious abuses and shorter review intervals. A recycled annual risk map becomes evidence against the company and affords it no protection.

04 **Focusing on motive at the expense of knowledge.** Under the judgment of 7 September 2021, a commercial motive does not negate the mental element of complicity. Knowingly paying an organisation whose purpose is exclusively criminal, in the knowledge of the crimes it is preparing or committing, suffices without endorsement of the criminal plan. The defence turns on what the company knew and when.

05 **Leaving intermediaries to "manage" matters on the ground.** Local arrangements handled by intermediaries without instructions or written reporting build the evidential case for a knowing contribution, document by document - while depriving head office of control over events.

06 **Providing material support to security forces with a known record of abuse.** Housing, equipping, transporting or paying units implicated in abuses without written conditions or traceability creates a risk of complicity and may reveal a breach of the duty of vigilance. Any such breach is assessed against the applicable obligations and the reasonable measures actually taken to address the known risk.

07 **Confusing certification with due diligence.** A certificate of origin, a label or membership of an industry scheme attests to a trading channel. None can replace mapping the actual chain, auditing its critical links or responding to alerts in stages.

08 **Ignoring a formal notice or allegation letter.** Silence leaves the opposing account alone on the public record and uses up the time - often brief - in which a documented response could still establish the company's position.

09 **Making statements without legal clearance.** Every public statement is potential evidence in criminal, civil and duty of vigilance proceedings. Implicit admissions, unfulfilled promises and contradictions across publications are systematically exploited.

10 **Combining the defence of the company with that of its executives.** Their interests can diverge as the investigation progresses. A single defence arrangement sets the stage for conflicts of interest that will emerge when it is too late to separate their positions.

11 **Exiting without assessing the exit.** A hasty withdrawal - an unaudited purchaser, employees left behind, remediation interrupted - can aggravate impacts and exposure and publicly contradict the earlier reasons for staying.

12 **Keeping records without discipline - or keeping none.** A lack of records may be read as concealment. Undisciplined records provide evidence for the opposing party. The only sound course is controlled documentation: accurate facts, signed analyses, reasoned decisions, recorded follow-up and long-term retention.

# What to expect from an initial discussion with Hennebel Avocats

The initial discussion with the firm is confidential, entails no commitment and is confined to assessing the situation. It typically lasts between forty-five and ninety minutes and takes place by secure telephone, encrypted videoconference or in person, depending on availability and where the matter is being handled. The firm uses Signal and Threema for confidential communications and a secure facility for sensitive documents. Substantive information must be sent only through dedicated channels.

The discussion covers three areas: the precise nature of the context and exposure (the area concerned, the entities and individuals exposed, and any matters already under way - allegations, formal notices, investigations or proceedings), the timeline of events and decisions already taken (sensitive transactions, incidents, public statements and the state of the records), and the preliminary strategy (applicable law, sequence of responses, coordination across fronts, and options for staying, suspending operations or exiting). Following the initial discussion, if the firm is in a position to act, it may offer a written assessment setting out the options, their recommended sequence and the possible scope of an engagement. The terms are specified before drafting begins.

The initial discussion is covered by legal professional privilege, subject to the conditions and limits prescribed by law, regardless of whether the matter proceeds further.

In a confirmed emergency - a search of premises, a criminal allegation against an executive, a serious incident at a site, an imminent board decision or a public allegation already circulating - the firm gives urgent requests priority and can activate a crisis team (Crisis Room · Praesidium) to coordinate the legal characterisation, preservation of evidence, governance and communications in parallel.

ANNEX - AUTHORITIES CITED

# Table of instruments and decisions cited

*Authorities cited throughout the guide and their practical takeaway. The main text explains their scope and limitations.*

| REFERENCE | SUBJECT | PRACTICAL TAKEAWAY |
|---|---|---|
| **UNGP, 2011** | United Nations Guiding Principles on Business and Human Rights (Human Rights Council resolution 17/4) | "Protect, Respect and Remedy" Framework. Principles 7 (conflict zones and the role of States), 12 (standards to be respected, with the commentary including IHL in armed conflict), 17 (due diligence, developed in Principles 18 to 21), 19 and its commentary (leverage and responsible disengagement), 22 (remediation), and 23 (treating the risk of causing or contributing to gross abuses as a legal compliance issue). |
| **UNDP, 2022** | Guide to heightened human rights due diligence in conflict-affected contexts (with the UN Working Group) | Method for heightened due diligence: conflict analysis, interactions between the company and the conflict, a lower threshold for action and responsible exit. |
| **OECD, 2023** | OECD Guidelines for Multinational Enterprises (2023 edition) | Standard for responsible business conduct (full title of the 2023 edition: OECD Guidelines for Multinational Enterprises on Responsible Business Conduct). Basis for the work of National Contact Points and their public final statements. |

| | | |
|---|---|---|
| **OECD, 2018** | OECD Due Diligence Guidance for Responsible Business Conduct | Six practical steps for due diligence. Reference framework for mandatory regimes. |
| **OECD, minerals (3rd ed.)** | OECD Due Diligence Guidance for Responsible Supply Chains of Minerals | Five-step framework and model policy annex distinguishing risks requiring an immediate response from those calling for graduated engagement. Standard incorporated by reference into Regulation (EU) 2017/821. |
| **Act No. 2017-399** | French Duty of Vigilance Act of 27 March 2017 (Commercial Code, Articles L. 225-102-1 and L. 225-102-2, formerly Articles L. 225-102-4 and L. 225-102-5). Case law: Paris Court of Appeal, 18 June 2024 (admissibility) and 17 June 2025. Paris Judicial Court, 12 March 2026 and 25 June 2026 (merits) | Vigilance plan, formal notice and action for an injunction (three-month period), and a liability action for harm that compliance with the duty of vigilance would have prevented. |
| **Dir. (EU) 2024/1760** | Directive of 13 June 2024 on corporate sustainability due diligence (CS3D) | The Union's duty of vigilance draws on the UN and OECD frameworks. Under the general regime for EU companies, Directive (EU) 2026/470 (Omnibus I) sets thresholds of more than 5,000 employees and more than EUR 1.5 billion in net worldwide turnover. Also check group thresholds, the rules for third-country companies and the separate route for franchising or licensing (step 01). Civil liability is governed by national law. Member States must transpose the directive by 26 July 2028 and, as a general rule, apply it from 26 July 2029. |

| | | |
|---|---|---|
| **Reg. (EU) 2017/821** | Conflict Minerals Regulation (tin, tantalum, tungsten and gold) | Due diligence obligations for Union importers aligned with the OECD Guidance: management systems, traceability and third-party audits. |
| **Reg. (EU) 2021/821** | Regulation on export controls for dual-use items | Export authorisations, catch-all provisions based on destination and end user, and controls on cyber-surveillance items. |
| **Court of Cassation, Criminal Chamber, 7 Sept. 2021** | Lafarge case (judgment quashed in part at the judicial investigation stage). Subsequent proceedings: Court of Cassation, Criminal Chamber, 16 Jan. 2024, No. 22-83.681 (formal investigation for complicity in crimes against humanity upheld). Paris Criminal Court, 13 Apr. 2026 (conviction for financing a terrorist enterprise, appeal pending as at 29 October 2026) | Knowingly paying several million dollars to an organisation whose purpose is exclusively criminal suffices to establish complicity in crimes against humanity. Endorsement of the criminal plan is not required. A commercial motive is immaterial. |
| **Rome Statute, Article 25(3)(c)-(d)** | Modes of liability: aiding and abetting, and contributing to the commission of a crime by a group | Scope of the risk of a punishable contribution - financing, supply or logistics - for executives and employees as natural persons. The company as an entity is subject to domestic criminal laws, since the ICC has no jurisdiction over legal persons. |
| **Kiobel, 2013 · Jesner, 2018 · Nestlé USA, 2021** | Narrowing the scope of the Alien Tort Statute (US Supreme Court) | Restrictions on extraterritorial application, exclusion of foreign corporations and insufficiency of domestic management decisions alone. US civil exposure persists on other grounds, and litigation is extending to Europe. |

| | | |
|---|---|---|
| **Common Article 3 · ICRC, 2006** | Article 3 common to the Geneva Conventions. ICRC study "Business and IHL" | Minimum rules of IHL applicable in non-international armed conflicts. Relevance of IHL to companies, their personnel, property and executives. |
| **Voluntary Principles, 2000** | Voluntary Principles on Security and Human Rights | Framework for relations with public and private security forces: risk assessment, dialogue with the authorities and incident management. |
| **Montreux, 2008** | Montreux Document on private military and security companies | Restatement of relevant international obligations and good practices for selecting, contracting with and overseeing providers in armed conflict. Complemented, for providers, by the International Code of Conduct for Private Security Service Providers and its association (membership, certification and reporting). |
| **Kimberley** | Kimberley Process (rough diamonds) | Intergovernmental certification of trading channels, with documented limitations - certification does not discharge the buyer's own due diligence responsibilities. |
| **Dir. (EU) 2024/1226** | Directive of 24 April 2024 on the definition of criminal offences and penalties for the violation of Union restrictive measures | Harmonised criminalisation of the violation and circumvention of restrictive measures, and liability of legal persons. Transposition was due by 20 May 2025. Check implementation in each State. |

| | | |
|---|---|---|
| **Reg. (EC) No. 2271/96 · CJEU, C-124/20** | Regulation blocking the extraterritorial application of third-country legislation. Bank Melli Iran judgment of 21 December 2021 | Prohibition on compliance without authorisation with the foreign regimes listed in the Annex. Termination without stating reasons is possible, but the operator must prove it had no intention to comply where the evidence indicates that it did. Termination may be annulled unless annulment would have disproportionate effects on the operator in light of the economic losses it faces. An application to the Commission for authorisation can assist the operator. |
| **Act No. 68-678 · Decree No. 2022-207** | Blocking statute of 26 July 1968. Procedure for notification to the Strategic Information and Economic Security Service | Requesting, seeking or disclosing information covered by Article 1 bis for the purposes of foreign judicial or administrative proceedings is punishable under criminal law, subject to applicable international treaties or agreements and the laws and regulations in force. Any request within the scope of the statute must be reported without delay. |
| **Code of Criminal Procedure, Articles 7, 56-1-2, 173-1, 175, 198 and 385 · Criminal Code, Article 434-4** | Limitation periods for prosecution, exceptions to privilege for legal advice, deadlines for raising nullities and filing submissions and at the close of the judicial investigation, and obstruction of the ascertainment of the truth | No limitation period for crimes against humanity, and a thirty-year period for war crimes. In searches and seizures, privilege for legal advice cannot be invoked against measures concerning the tax offences in Articles 1741 and 1743 of the General Tax Code, terrorist financing, the offences exhaustively listed in Articles 433-1, 433-2 and 435-1 to 435-10 of the Criminal Code, or laundering the proceeds of those offences, where the documents establish that they were used to commit or facilitate the offence. Grounds of nullity must be raised within four months (Article 173-1 as amended by Act No. 2026-651 of 23 July 2026, applicable to applications made on or after 23 October 2026). Following notice of completion of the judicial investigation, requests and applications must be made within one or three months, subject to the separate time bars for invoking a limitation period that has already expired (Article 82-3) and for raising nullities (Article 173-1). Supplementary observations may be submitted in the following ten days (Article 175). Subject to exceptions, written submissions |

| | | |
|---|---|---|
| **Act No. 2026-122** | Act of 23 February 2026 on the confidentiality of legal advice given by in-house counsel | Confidentiality may be invoked from 1 January 2027 subject to the statutory requirements concerning qualifications, training, intended recipients, marking and filing. It cannot be invoked in criminal or tax matters (Decree No. 2026-1054 of 17 November 2026, Article 12). |
| **Foreign proceedings cited** | United States v. Lafarge S.A. and Lafarge Cement Syria (guilty plea, 18 October 2022). Kashef v. BNP Paribas (S.D.N.Y., verdict of 17 October 2025). Lundin Oil trial (Stockholm District Court) | US criminal and civil exposure persists despite the narrowing of the ATS. In Sweden, executives face prosecution and the prosecution has sought confiscation from the company (judgment initially expected on 3 December 2026, then postponed to 17 February 2027 by announcement of 30 October 2026). The status of the other proceedings is given as at 29 October 2026. |
| **UN Working Group, A/75/212 (2020)** | Report of the Working Group on Business and Human Rights to the General Assembly (conflict-affected contexts) | Formulation of heightened due diligence derived from Principle 7: conflict analysis, interaction between the company and the conflict, prioritisation that takes conflict risk into account, and responsible exit. |
| **Special procedures, A/HRC/58/70 (2025)** | Report on the activities of the special procedures in 2024, submitted to the Human Rights Council | Communications are published sixty days after dispatch (forty-eight hours for letters concerning legislation, a policy or a practice), together with responses received. Check the practice at the time of response. |

# Main sources

- United Nations Guiding Principles on Business and Human Rights (2011), endorsed in Human Rights Council resolution 17/4, in particular Principles 7, 12, 17 to 22 and 23.
- United Nations Working Group on Business and Human Rights, report to the General Assembly on business, human rights and conflict-affected contexts (A/75/212, 2020). UNDP and the Working Group, guide on heightened human rights due diligence in conflict-affected contexts (2022). Report on the activities of the special procedures in 2024 (A/HRC/58/70, 2025).
- OECD Guidelines for Multinational Enterprises on Responsible Business Conduct (2023). OECD Due Diligence Guidance for Responsible Business Conduct (2018). OECD Due Diligence Guidance for Responsible Supply Chains of Minerals from Conflict-Affected and High-Risk Areas (3rd edition).
- Act No. 2017-399 of 27 March 2017 on the duty of vigilance of parent companies and contracting companies (Commercial Code, Articles L. 225-102-1 and L. 225-102-2, formerly Articles L. 225-102-4 and L. 225-102-5). Code of Judicial Organisation, Article L. 211-21. Paris Court of Appeal, 18 June 2024 (Nos. 23/14348, 21/22319, 23/10583) and 17 June 2025. Paris Judicial Court, 12 March 2026 (RG 22/04017) and 25 June 2026 (RG 22/03403).
- Directive (EU) 2024/1760 of 13 June 2024 on corporate sustainability due diligence, as amended by Directive (EU) 2026/470 of 24 February 2026 (Omnibus I).
- Regulation (EU) 2017/821 (conflict minerals). Regulation (EU) 2021/821 (dual-use items). Directive (EU) 2024/1226 on the definition of criminal offences and penalties for the violation of Union restrictive measures. Regulation (EC) No. 2271/96 of 22 November 1996 protecting against the effects of the extra-territorial application of legislation adopted by a third country (Blocking Regulation) and CJEU, 21 December 2021, Bank Melli Iran, C-124/20. Act No. 68-678 of 26 July 1968 (the French blocking statute) and Decree No. 2022-207 of 18 February 2022.

- Court of Cassation, Criminal Chamber, 7 September 2021, No. 19-87.367 (Lafarge case, judgment quashed in part). Court of Cassation, Criminal Chamber, 16 January 2024, No. 22-83.681. Paris Criminal Court, 13 April 2026 (under appeal). Code of Criminal Procedure, Article 56-1-2 (limits on invoking privilege for legal advice), Article 7 (limitation periods for prosecution) and Articles 173-1, 175, 198 and 385 (deadlines for raising nullities and at the close of a judicial investigation), as amended in particular by Act No. 2026-651 of 23 July 2026, article numbers in force on 29 October 2026. The Code is being recodified under Ordinance No. 2025-1091 of 19 November 2025, effective 1 January 2029. Criminal Code, Article 434-4. Act No. 2026-122 of 23 February 2026 (confidentiality of legal advice given by in-house counsel).
- US Supreme Court: Kiobel (2013), Jesner (2018), Nestlé USA v. Doe (2021) - narrowing the scope of the Alien Tort Statute. United States v. Lafarge S.A. and Lafarge Cement Syria (guilty plea, 18 October 2022). Kashef v. BNP Paribas (S.D.N.Y., verdict of 17 October 2025, under appeal). Sweden, trial of two former Lundin Oil executives (Stockholm District Court, hearings concluded on 28 May 2026).
- Rome Statute of the International Criminal Court, Article 25(3)(c) and (d).
- Article 3 common to the Geneva Conventions of 1949. ICRC study "Business and International Humanitarian Law" (2006).
- Voluntary Principles on Security and Human Rights (2000). Montreux Document (2008). International Code of Conduct for Private Security Service Providers.
- Kimberley Process (certification of rough diamonds).

**Verification.** The law is stated as at 21 November 2026. References were checked on that date against the instruments and decisions cited.

# Keywords

business and human rights · conflict zone · heightened due diligence · 2011 Guiding Principles · duty of vigilance · Act 2017-399 · CS3D · CSDDD · Omnibus I · formal notice under the duty of vigilance · vigilance plan · criminal complicity · Lafarge case · Rome Statute · crimes against humanity · Alien Tort Statute · Voluntary Principles · Montreux Document · conflict minerals · OECD Guidance · National Contact Point · sectoral sanctions · dual-use items · responsible exit · remediation · crisis governance · Hennebel Avocats

# Hennebel Avocats

Pr. Ludovic Hennebel

global@hennebel.legal

**To cite this document**

Ludovic Hennebel, 'Companies in conflict zones: a practical guide' (Praxis, Hennebel Avocats 2026) <https://hennebel.legal/en/praxis/guide-entreprises-situations-exceptionnelles> accessed November 24, 2026.

Generated on November 24, 2026