



# ADDRESSING RISKS OF RETALIATION IN THE FORTHCOMING EU DIRECTIVE ON MANDATORY DUE DILIGENCE



Tove Holmström

## About the author

A former staff member of the UN Human Rights Office, Tove Holmström is an independent consultant based in Paris, France. Her work addresses responsible business conduct, with a particular focus on retaliation against stakeholders. In this field, she has worked with the Organization for Economic Co-operation and Development (OECD), the Independent Consultation and Investigation Mechanism of the Inter-American Development Bank, the Project Complaints Mechanism of the European Bank for Reconstruction and Development, IDB Invest and the UN Special Rapporteur on the situation of human rights defenders. From 2018 to 2020, she served as an independent expert at the internal accountability mechanism of the French Development Agency (Agence Française de Développement).

She can be reached at [tove.holmstrom@multi.fi](mailto:tove.holmstrom@multi.fi)

## Executive summary

As a result of growing societal expectations on companies to avoid causing or contributing to harm, including across their global supply chains, public engagement and reporting by company employees or other stakeholders, including local activists or non-governmental organizations, on companies' due diligence practices has increased. Engagement with companies – through stakeholder engagement, public reporting, lawsuits or advocacy campaigns, for example – have in many instances resulted in retaliation against those that report. Such retaliation has encompassed a broad range of acts, including verbal intimidation, slander and defamation, strategic lawsuits against public participation, electronic or physical surveillance, property damage or loss, restrictions to freedom of movement, travel bans, physical attacks leading to bodily harm or fatality, and discrimination, disadvantage or adverse treatment in relation to employment.

As a problem, retaliation is global: attacks take place within the EU and outside the EU, and perpetrators include EU-based companies and their business relationships domiciled elsewhere. In short, retaliation against stakeholders is at issue for all companies, across all sectors and across all countries. A premise for the current submission is that reprisals are expected to increase, both in numbers and gravity. This prediction is based on the current state of play for civil society, which at present is largely characterized by a rapidly deteriorating security environment.

Retaliation not only devastates the lives of the individuals concerned and their families, it but can also have serious reputational, financial and potentially legal risks for the companies implied. Stakeholders' concerns for their own and for their families' safety and wellbeing can also prevent them from voicing concerns over anticipated or experienced impacts associated with companies' activities. If fear of retaliation deters stakeholders from speaking freely about issues of concern to them, potential risks and impacts associated with companies' activities may go unnoticed and, where such risks and impacts materialise, can lead to increased costs and delays in implementation for companies due to unanticipated problems.

Under the proposed EU directive on mandatory due diligence for companies, civil society – including individuals and organizations – will have a key role to play to monitor companies' compliance with the directive – whether through direct engagement with the companies concerned in the context of stakeholder engagement, through media reporting, lawsuits, public advocacy campaigns or by engaging with designated enforcement or monitoring authorities. But in doing so, civil society will also face genuine risks of retaliation. Because of this, the EU Commission will need to consider how to address these risks upfront through the Directive – set to be tabled in 2021 – and any associated procedural guidance for companies and Member States.

This submission seeks to address how the forthcoming EU Directive and any associated guidance could address risks of retaliation to ensure that civil society – individuals, communities and organizations working from both within and outside the EU – can safely report on companies' (mis)conduct to support the effective implementation of the Directive. More specifically, it considers the following questions:

1. How can the Commission place a negative obligation on companies to not retaliate against stakeholders?
2. How can the Commission encourage companies' to take appropriate steps to identify, prevent, cease, mitigate and monitor risks of retaliation against a broad range of stakeholders,

account for how these have been managed (with due regard for any concerns to personal safety) and, as relevant, remediate instances of retaliation that have occurred?

3. Should the Commission, in the legislative proposal and/or associated procedural guidance, tie any specific references to retaliation to other directives and policies at the EU level, such as, for example the Whistleblower protection directive (2019)?
4. What can the EU, as an institution, do to reduce risks of reprisals by companies against stakeholders both within and outside the EU, and to respond to instances of retaliation that have occurred?
5. What can the EU ask Member States to do to prevent and appropriately manage risks of retaliation, and respond to retaliation that has occurred? More specifically, in terms of enforcement of the Directive by Member States, how can risks of retaliation best be considered and what positive/negative obligations and guidance can the Commission give Member States in this regard? In particular, what guidance should be given on the type and level of proof that should be presented and by whom to determine if companies have been implied in retaliation by virtue of their acts or omissions or in relation to the acts or omissions of their business relationships?

The practical suggestions that conclude this submission have been informed by how risks of retaliation have been addressed in other contexts – including by the private sector, multilateral organizations and governments with existing due diligence and/or reporting requirements for companies.

<b>Executive summary</b> .....	2
<b>Overview of recommendations</b> .....	5
<b>What’s the issue?</b> .....	9
<b>Why is addressing risks of retaliation important?</b> .....	13
<b>Current protections afforded against retaliation at the EU-level</b> .....	14
<b>How have risks of retaliation been reflected to date in due diligence initiatives?</b> .....	19
Due diligence initiatives at the national level .....	19
EU-adopted supply chain due diligence initiatives.....	21
<b>How are risks of retaliation reflected in current discussions over the proposed directive?</b> .....	22
<b>How to reflect risks of retaliation in a coherent manner in the Directive: practical suggestions and recommendations</b> .....	25
<b>References</b> .....	29

## Overview of recommendations

1. **Pro-actively communicating zero-tolerance to retaliation to companies is one of the most – if not the most – effective measure to prevent retaliation.** At a minimum, the Directive itself should recognize that stakeholders, including local communities, individuals and organisations working to expose business-related environmental, human rights and governance risks and harms, trade unionists and worker representatives – are important sources of information for companies' due diligence processes, and that companies should respect their right to freely express their opinions and views – including critical – at all times. It should recognize that the individuals, communities and organisations that raise concerns or otherwise address risks and impacts associated with companies' operations and activities, or those of their business relationships – can face genuine risks of retaliation for doing so, and place **a negative obligation on companies to not take acts in reprisals or sanction acts of reprisals taken by business relationships**. The Directive should define reprisals as any detrimental action that impairs or harms, or threatens to impair or harm, anyone seeking to, or having, expressed opinions, concerns, or opposition to a company's activities or to the activities of its relevant business relationships, and that the types of acts that the umbrella term retaliation covers can include, but are not limited to any, or a combination of, intimidation and threats, slander and defamation, strategic lawsuits against public participation, electronic or physical surveillance, property damage or loss, physical attacks leading to bodily harm or fatality, or discrimination, disadvantage or adverse treatment in relation to employment.
2. The Directive should also place a **positive obligation on companies to prevent retaliation. This would entail that companies should, as part of their due diligence, be required to seek to ensure that all stakeholders – including those with critical views – can express their views in a manner that does not cause them, or others associated with them, any harm.** More specifically, as part of their due diligence and enabling access to remedy, companies should be expected to identify, assess and prioritize risks of retaliation against stakeholders and to put in place any measures needed to prevent, mitigate or otherwise address these risks depending on their level of involvement (cause, contribute to, directly linked to), in collaboration with those concerned. This can include, amongst other, proactively including references to zero-tolerance to retaliation in commercial contracts with business partners and requesting that these requirements be cascaded down to the next part in the supply chain and otherwise communicating this expectation to business relationships including State authorities, ensuring safe channels for those at risk to communicate any concerns they have about their safety, and enabling victims of retaliation to seek remedy to restore them to their original situation had harmed (retaliation) not occurred.
3. If liability is reflected in the Directive, this submission recommends that **criminal liability – corporate and individual – should be an option in cases where companies have been found to have caused or can reasonably, in all the circumstances of the situation at hand, be considered to have contributed to severe forms of retaliation (such as, for example, bodily harm or fatalities).** National legislative frameworks on corruption – notably the UK Bribery Act (2010) – can provide a useful model in this regard (liability for the failure to prevent, coupled with the defence of having put in place adequate prevention procedures). More specifically, in terms of severe forms of retaliation, it is recommended that **criminal liability be linked to companies' failure to prevent retaliation by associated persons to impair or harm anyone seeking to, or having, expressed opinions, concerns, or opposition to a company's activities or to the activities of its business relationships.**<sup>i</sup> To ensure that remedy for those that have

**suffered the retaliation is not out of reach, a provision on civil remedy for damages should also be reflected in the Directive.**

4. With the understanding that the Directive itself will not provide particular guidance on thematic risks that can have an impact on, or be particularly relevant for, companies' due diligence processes, the **Directive could refer to forthcoming implementation guidance** for companies and Member States **and note that safe stakeholder engagement in general, and risks of retaliation in particular, will be further elaborated in these with actionable examples.**
5. The current protections afforded by EU Directives to the different groups that are typically subject to reprisals for addressing corporate misconduct currently form a haphazard and uneven patchwork, and it is unclear to what extent existing directives could be relied on to prevent retaliation or to address retaliation that has occurred. **Should the Commission choose to refer to Directives like the Whistleblower protection directive, it should be made clear at the outset that additional measures should be taken by both companies and member states to prevent, mitigate and respond to risks of retaliation and address instances of retaliation that have occurred against a broader group of stakeholders than those that could potentially enjoy a certain degree of protection under the Whistleblower protection directive for reporting corporate misconduct.** More broadly, the European Commission's ongoing work to develop a legislative or non-legislative initiative on action to protect journalists and civil society against strategic lawsuits against public participation in the last quarter of 2021 remains particularly important and **could be cross-referenced in the directive on mandatory human rights due diligence and in any associated guidance.**
6. In addition, the Commission is advised to initiating work to develop **legislative or non-legislative initiatives to expand current source protection (source confidentiality)** – the right accorded to journalists under international law and certain national legal frameworks to not disclose the identity of their sources – **to also include other professionals, in particular non-governmental organizations, to be able to invoke the right to source protection when bringing business and human rights claims against companies in front of national courts of law.** Without a strong guarantee of anonymity, many NGOs that are working to bring complaints have decided not to do so because courts have been unable, or unwilling, to expand this protection to the original claimants or to those that have provided crucial information needed to initiate proceedings.
7. **With regards to Member States' enforcement of the Directive on mandatory due diligence through the transposition into national law, the Directive should include particular consideration of, and reference to, risks of retaliation and how these will be managed by Member States, including by any designated authorities that will oversee the enforcement of the Directive.** Addressing risks of retaliation should entail going beyond simply granting potential complainants the right to remain anonymous.<sup>ii</sup> In particular, identifying and managing risks of retaliation should be considered, and cross-referenced for the following:
  - In terms of any effective, proportionate and dissuasive penalties, including civil and criminal, that the directive will propose, as has been noted, this submission recommends that **criminal liability – corporate and individual – should be an option in cases where companies have been found to have caused, or can reasonably, in all the circumstances of the situation at hand, be considered to have contributed to, severe forms of retaliation (such as, for example, bodily harm or fatalities) against stakeholders that have voiced concerns over their activities or those of their business partners and been subject to harm because of that.** National legislative frameworks on corruption – notably the UK Bribery Act (2010) – can provide a useful model in this regard (liability for the failure

to prevent, coupled with the defence of having put in place adequate prevention procedures). In terms of severe forms of retaliation, it is recommended that **liability be linked to companies' failure to prevent retaliation by associated persons to impair or harm anyone seeking to, or having, expressed opinions, concerns, or opposition to a company's activities or to the activities of its business relationships.**<sup>iii</sup> The complex question of responsibility for retaliatory actions of companies' business relationships in their supply chain should be determined by a court, with reference to reasonableness of the due diligence undertaken, including leverage exercised in the relevant circumstances. **To ensure that remedy for those that have suffered the retaliation is not out of reach, a provision on civil remedy for damages should also be reflected in the Directive. As such, having suffered retaliation should in itself be sufficient grounds for victims to bring cases in front of national courts of law.**

- Where **instances of retaliation have been reported**, and in line with established practice in the field of whistle-blower protection, Member States should establish that the **burden of proof falls on the company**, not on the individual or group that claim to have been subject to retaliation. In other words, where companies are alleged to have caused or contributed to retaliation, companies should be requested to present evidence to the contrary, and that adequate prevention has been put in place to reduce risks of retaliation, through the conduct of appropriate due diligence that is proportionate to the identified level of risk.
- When establishing enforcement rights and procedures for interested parties, the **designated authority or authorities** that may supervise the proper enforcement of the Directive should **have dedicated policies on how to protect individuals (complainants or others) from retaliation for submitting complaints or otherwise engaging with companies to express concerns over risks or impacts that they have caused, contributed to or been directly linked to.** Such policies should go beyond merely granting the right to anonymity of complainants, and should include proactive risk assessments and the development of risk mitigation measures, in consultation with those concerned.
- If providing **competent bodies the right to investigate abuses, initiate enforcement actions and support victims**, appropriate procedures should be developed to identify and effectively manage risks of retaliation, in close consultation with those concerned. This requires that staff of the competent bodies have the **right set of skills and protocols in place and the possibility to collaborate with other actors, including in a cross-border context, to mitigate and address risks. As appropriate, competent bodies should have within their "toolbox" the option to also take steps to protect persons at risk in countries outside the EU**, such as by working with police teams in the countries concerned, where victims have agreed to doing so and would not expose them to further risks.
- When facilitating and providing effective means of remedy for victims (including judicial and non-judicial remedies), member states should **encourage companies to put in place appropriate grievance mechanisms that can be accessed by potential complainants without exposing them to risks of retaliation**, including by, for example accepting anonymous submissions, or by collaborating with other actors, such as, for example, independent national human rights institutions, to accept complaints linked to their activities or business relationships in challenging contexts. Companies should be encouraged to **assess to what extent the grievance mechanisms run by multi-stakeholder initiatives in which they participate can ensure safe access and the safe handling of complaints** for complainants and others associated with them or the complaints handling process. At the **national level, grievance mechanisms – including for example National**



**Contact Points – should also be strengthened to ensure safe access. In liability claims, retaliation should in itself constitute sufficient grounds for lawsuits. Where retaliation is found to have taken place, Member States should consider granting victims within the EU access to national criminal compensation schemes to help repair the harm that they have suffered.**

## What's the issue?

In recent years, reports of retaliation<sup>iv</sup> against individuals, communities and organisations that express concerns about business-related risks and impacts have increasingly made international headlines.<sup>v</sup> These reports take place against a global backdrop of rapidly shrinking civic space. In 2018, for example, CIVICUS concluded that civic space was under attack in 111 of the world's countries – well over half – and that only 4 per cent of the world's population lived in countries where fundamental civil society freedoms – of association, peaceful assembly and expression – were fully respected.<sup>vi</sup> In 2021, serious restrictions on civic space on every continent continues to be a widespread challenge.

Concern for this shrinking civic space has been expressed by the European Commission, with regular statements being made on country-specific situations.<sup>vii</sup> At both central and delegation level, the EU also continues to deliver various demarches, both through informal and formal channels, on behalf of victims of retaliation, asking for their release and condemning reprisals and attacks against.<sup>viii</sup> In some instances, the EU has also imposed targeted restricted measures against countries for repression and crackdown on civil society.<sup>ix</sup> In February 2020, the Council of the EU adopted conclusions on the Union's priorities in UN fora, affirming that that the EU would continue to promote the implementation of the UN Guiding Principles on Business and Human Rights both in its external action and internal policies, including through support to environmental and indigenous human rights defenders.<sup>x</sup>

Increasingly so, there is credible information to suggest that companies – either through their own actions or omissions or by virtue of their association with commercial business partners and other business relationships – are implied in acts of retaliation against individuals or groups that seek to bring attention to business-associated risks and impacts. As has been noted in the background study requested by the European Commission, acts of retaliation by companies is increasingly such a widespread issue that the Business and Human Rights Resource Centre has an entire portal dedicated to tracking and documenting examples of attacks on human rights defenders in the context of business activity.<sup>xi</sup> Similarly, a background briefing requested by the European Parliament also highlight that victims of corporate misconduct continue to face legal and practical obstacles to access to justice and effective remedy, including attacks on human rights defenders, victims, witnesses, lawyers, judges and journalists and the risk of counter-litigation.<sup>xii</sup>

Retaliation against individuals, communities and organisations that seek to address business-associated risks and harms is a global problem. This means that reprisals can be taken, encouraged or sanctioned by companies in practically any country – inside the EU and in non-EU countries.

Companies domiciled in the EU are also increasingly operating in markets where contextual risk factors render both likelihood and severity of retaliation against stakeholders high for raising their concerns.<sup>xiii</sup> In these contexts, conducting meaningful stakeholder engagement, as required by international standards on responsible business conduct, may not be possible at all. In these contexts, companies may also find themselves directly linked to such acts by virtue of their business relationships with third parties, including governments.



**Companies domiciled in EU Member States are increasingly operating in markets where contextual risk factors render both the likelihood and severity of acts of retaliation against stakeholders high. In these contexts, conducting meaningful stakeholder engagement, as required by international standards on responsible business conduct, may not be possible at all.**

As with any (potential or actual) adverse impacts, companies can cause, contribute to or be directly linked to retaliation.<sup>xiv</sup> Common perpetrators of retaliation include:

- Companies domiciled in EU Member States or under their jurisdiction.
- Companies not domiciled in /under the jurisdiction of EU Member states but providing products and services to the EU internal market.
- The direct and indirect business partners of companies, including, but not limited to, clients, portfolio companies, contractors and sub-contractors, suppliers and sub-suppliers, consultants and sub-consultants.
- Other business relationships, in particular State authorities or actors associated with them (such as, for example, public security forces) that provide services deemed necessary for the operations and activities of companies or their business partners.
- Members of the same community as the victim or victims. This is particularly at issue in contexts where communities are divided over the prospect of a business activity.

The following categories or groups are particularly at risk of reprisals:

- Communities or individuals directly impacted by a company's potential or actual adverse impacts, in particular community leaders and their family members.
- Individuals or organisations working with project impacted communities to bring attention to adverse impacts, such as civil society organizations and lawyers.
- Journalists reporting on corporate misconduct.
- Requesters to project level grievance mechanisms or to higher-level independent accountability mechanisms and local consultants, including interpreters, consultants and drivers, that facilitate the work of such mechanisms.
- Members of the company's workforce, including workers hired by contractors, sub-contractors, suppliers and sub-suppliers and consultants and sub-consultants that express concern over work-practices associated with the project, in particular through workers' organisations (workers active in trade unions).

Some of the individuals, communities or organizations that suffer retaliation for trying to expose business-related risks and impacts may already be publicly pursuing human rights advocacy in their countries and be at high risk of reprisals because to that. As such, the risks they face for this work and those they face for trying to engage with specific companies are easily blurred. Nevertheless, engaging with companies or trying to raise concerns over specific risks and impacts associated with their activities typically aggravates existing risks.

The table below provides an illustrative overview of the types of retaliatory acts that companies cause, contribute to or be directly linked to through the operations, products or services by business relationships.<sup>xv</sup>

**Table 1. Illustrative examples of companies' involvement in retaliation and links to the EU**

<i>Type</i>	<i>Example</i>	<i>Victim</i>	<i>Victim(s) located in</i>	<i>Perpetrator</i>	<i>Perpetrator domiciled in</i>	<i>Link to EU</i>
Physical attacks	Violent attacks against local communities and NGO supporting them to raise concerns over impacts associated with rubber plantations.	Local community members	Liberia	Local contractor of EU-based entity with palm and rubber plantation operations and marketing of oil palm seeds	Liberia	Perpetrator is a company owned by EU-based multinational.
Destruction of property	Destruction of computers at office following targeted break-in, burning of vehicles.	Community-based organisation	Cambodia	Sugar cane plantation company	Cambodia	Company provides sugar to EU market based on preferential trade scheme
Torture	Torture, mass firings and trials in military courts	Trade unionists and civilian workers organizing strikes at shipyard	Egypt	Central government authority	Egypt	Goods manufactured at the shipyard have been ordered by and provided to company domiciled in EU Member State.
Strategic lawsuits against public participation	A series of lawsuits brought by a European construction company against a small NGO. According to the lawsuits, the NGO has violated the company's presumption of innocence when filing a complaint alleging that the company and its executives, belonging to their foreign subsidiary, were responsible of having conducted forced labour, reduction to servitude and concealment. The lawsuits demanded damages amounting to several hundred	NGO	France	Company that is alleged to, through a foreign subsidiary, rely on forced labour in operations outside of EU	France	Multinational domiciled in EU Member State.

<b>Type</b>	<b>Example</b>	<b>Victim</b>	<b>Victim(s) located in</b>	<b>Perpetrator</b>	<b>Perpetrator domiciled in</b>	<b>Link to EU</b>
	thousand euros from employees of the NGO.					
Assassination	Murder of indigenous and environmental rights campaigner opposing a hydroelectric project.	Community leader	Honduras	Dam construction company	Honduras	Perpetrator associated with portfolio company receiving direct funds from two EU-based multinationals.
Surveillance	Interception of on-line communication. Government in country where civic space is under pressure contracts services of private digital surveillance companies to develop technology for the targeted digital surveillance of local activists and investigative journalists.	Reporters working to expose corruption in mining industry	Multiple	Private IT companies based in European countries.	Multiple	Companies providing software based in EU Member States.
Interruptions to financial services	Cancelling of accounts of local activists based on spurious claims of association with terrorists.	Local activists working to address impacts of a financial investor	Multiple	Bank	Multiple	Institutional investor based in EU.
Discrimination in relation to employment	Workers fired and black-listed for seeking to form independent trade union at factory level.	Trade unionists	China	Garment and footwear sector factory	China	Perpetrator in commercial relationship (first tier supplier) with EU based multinational.

## Why is addressing risks of retaliation important?

Addressing risks of retaliation in the EU Directive and associated procedural guidance for companies and for member states is important for a number of reasons, including:

- Civil society will have a key role to play to provide information on corporate misconduct under the new directive, and such information can lead to the effective detection and investigation of violations of EU law that would otherwise remain hidden and cause harm to the public interest. Experience shows that individuals are unlikely to provide this information in the absence of any measures to protect them against retaliation.<sup>xvi</sup>
- A failure to identify and appropriately manage risks of retaliation can have serious consequences for the safety of impacted individuals or communities.
- Under international standards on responsible business conduct that require companies to, at a minimum, respect the rights enshrined in the International Bill of Human Rights, companies are expected to respect the right of stakeholders' to freely express their views.
- Acts of retaliation often unfold in contexts where impacted individuals and communities have limited possibilities to express dissenting views and may be routinely punished for doing so. In these contexts, it is unlikely that key due diligence requirements – in particular meaningful stakeholder engagement – can be met.
- Individuals and groups that provide information on companies' operations, products or services can be an invaluable source of information for companies' due diligence processes – in particular for identifying, assessing and prioritizing risks and impacts. This is the case for both downstream and upstream impacts over which companies may have limited visibility.
- Where fear of retaliation deters individuals or organizations from speaking freely, risks and impacts associated with business activities may go unnoticed, and where such risks and impacts materialise, they can lead to increased costs and delays in implementation due to unanticipated problems.
- Where companies are associated with grave acts of retaliation – whether through their own acts or those of their business relationships – they may be subject to reputational, financial, and potentially legal repercussions.
- Communicating zero tolerance to retaliation against stakeholders – in particular those with diverging views – is increasingly considered good practice in the private sector.<sup>xvii</sup>
- Addressing risks of retaliation is a matter of policy coherence for the EU, including, amongst other, between Directive 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union Law and the European Union Guidelines on Human Rights Defenders.

## **Current protections afforded against retaliation at the EU-level**

To some extent, the protection against retaliation for reporting corporate misconduct has already made its way onto the EU's agenda, and some of the EU's existing Directives, initiatives and policies could be relied on for protection against some of the groups that face particular risks of reprisal. For example, depending on how the EU's Whistleblower-protection directive is transposed into national law by member states, protection could be afforded some individuals for reporting on corporate misconduct across supply chains. Directives establishing a requirement for informing and consulting employees could offer a certain degree of protection for employees based in the EU and performing their functions as worker representatives. The EU's Human Rights Defender Guidelines and associated funding mechanism could support others that are at imminent risk or that have suffered harm for disclosing companies' adverse impacts. Nevertheless, the current protections afforded to the different groups that are often subject to reprisals for speaking out against corporate misconduct – including across supply chains – currently form a haphazard and uneven patchwork.

### **Blowing the whistle: whistle-blower protection**

In recognition of the fragmented level of protection afforded to whistle-blowers at the European and national level, the European Commission presented, in April 2018, a package of initiatives including a Proposal for Directive on the protection of persons reporting on breaches of Union law and a Communication, establishing a comprehensive legal framework for whistle-blower protection for safeguarding the public interest at European level. This Directive was adopted in 2019 as Directive 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union Law (in short, the Whistleblower protection directive, or the Directive). Member States are expected to incorporate this directive into national law no later than December 2021. Until then, they are bound to transpose the Directive and are expected to refrain from any measures compromising its effectiveness.

The Whistleblower protection directive reinforces corporate compliance with EU law and sets the minimum standards for the protection of persons reporting breaches of Union law in the public and private sectors.<sup>xviii</sup> Protection applies to reports of wrongdoing relating to EU law in 12 policy fields: public procurement, financial services, products and markets, prevention of money-laundering and terrorist financing, product safety and compliance, transport safety, protection of the environment, radiation protection and nuclear safety, food and feed safety, animal health and welfare, public health, consumer protection, protection of privacy and personal data, and security of network and information systems. In addition to these defined fields, the EU has encouraged Member States to extend this protection to also cover wrongdoings relating to national law.

The Directive seeks to ensure accessible and confidential reporting channels for whistle-blowers and protect them from retaliation for making, or seeking to make, disclosures. This protection extends beyond the traditional conception of whistle-blowers (as employees working at the organisation at the time of reporting) by also including volunteers, paid or unpaid trainees, contractors, subcontractors and suppliers, individuals who disclose breaches during a recruitment process and former workers. The protection can also be invoked by facilitators, colleagues or relatives of the reporting person who are also in a work-related connection with the reporting person's employer or customer or recipient of services. Those that are self-employed, shareholders, management, and working with administrative or supervisory bodies would equally be covered.

If an individual reports in good faith and has reasonable grounds to believe that the information reported was true at the time and falls within the scope of the Directive, he or she would enjoy protection from any act or omission that causes detriment, whether direct, indirect, threatened, taken, recommended or even tolerated. Specifically, whistle-blowers are protected against termination of employment, negative impacts on promotions or salary, unjustified negative performance assessments, transfers and changes of workplace, and harassment or discrimination. The Directive imposes criminal, civil or administrative penalties on those who engage in retaliation. Importantly, in the case of allegations of reprisals, the burden of proof falls on the company, not on the whistle-blower.

*Depending on how Member States decide to transpose this Directive into their national laws, the whistle-blower protection directive could grant protection from retaliation to employees and the other categories covered (job applicants, former employees, supporters of the whistle-blower and journalists). This is particularly the case because the EU has encouraged Member States to protect these groups from reprisals for reporting on wrongdoings of national law, which the Directive on mandatory human rights due diligence will be also be incorporated into if/once adopted by the EU. As it stands, however, it is not likely that the Whistleblower protection directive could be relied on for offering any protection against retaliation against other stakeholders than those already covered by it (with a focus on employee-employer relationships and those associated with the whistle-blower). As such, it could not be relied on to identify, manage and respond to risks of retaliation against stakeholders that are typically at most risk for reporting corporate misconduct: individuals, communities and organizations that are not directly associated with the company by virtue of current, past or potential employment relationships, but that nonetheless expose companies' adverse impacts on human rights.*

#### **Informing and consulting workers: worker representatives**

In terms of the protection of worker representatives, Directive 2002/14/EC marked the introduction of workers' general right to information and consultation for the first time through standing structures across the European Union. Its *raison d'être* is to ensure that there are adequate procedures for employees to be informed and consulted whenever their employer intends to take serious decisions that may impact them, in particular in situations of potential restructuring. In terms of reprisals risks, the Directive requires Member States to ensure that employees' representatives enjoy adequate protection when carrying out their functions<sup>xix</sup>, without making any specific references to what such protection could be.

Directive 2009/38/EC, for its part, concerns the establishment of work councils for the purpose of information and consultation in companies that operate transnationally within the EU. These work councils – which are to be established in all companies meeting a certain threshold of employees and operating in more than one EU country – serve to keep workers informed and consulted by management about the development of the company's activity and any important EU-level decisions that may affect their working or employment conditions. The Directive establishes that employees' representatives acting within the framework of the Directive should not be subject to any discrimination as a result of the lawful exercise of their activities and should enjoy adequate protection as regards dismissal and other forms of sanction.<sup>xx</sup>

Council Directive 2001/86/EC governs the involvement of employees in European public-liability companies. It requires the establishment of arrangements for the involvement of employees in each such company in decisions on the strategic development of such companies. In terms of risks of



reprisals, it requires that protection be ensured those that exercise their function under the information and consultation procedure.<sup>xxi</sup>

*While these Directives remain relevant for employees working for companies that are operating within the EU community it does not extend the scope to supply chain workers (through including, within the scope of the directive, upstream suppliers, subcontractors and dependent companies downstream, for example). It is also unlikely that the Directives could be relied on for protection against retaliation against worker representatives for having exposed, or seeking to expose, supply chain risks and impacts that are typically addressed by supply chain due diligence requirements or occurring in production sites located outside of the EU internal market.*

### **Others that support victims of corporate harm or that work independently to expose corporate misconduct**

Retaliation against individuals or organizations that support victims of corporate harm or that work independently to expose corporate misconduct are also among common victims of reprisals for doing so. In this category, **non-governmental organizations (NGOs)** have been particularly exposed to retaliation in the form of strategic lawsuits against public participation (SLAPPs). For NGOs, defending cases against powerful corporate interests in court requires using a considerable proportion of their human resources, can paralyze their activity and entails significant financial risks, which can even result in their bankruptcy.<sup>xxii</sup> The variety of legal instruments applied to silence public participation is wide and not always related to freedom of expression. They most typically include defamation, criminal defamation, labour sanctions (dismissal), criminal charges of tax fraud and tax-audit procedure.<sup>xxiii</sup> Procedural rules may also be abused to prolong the procedure and exhaust the speaker.<sup>xxiv</sup>

At present, there is no anti-SLAPP legislation in force in any EU Member State. In June 2020, 119 NGOs called on the EU to protect freedom of expression and information by acting to end the use of SLAPPs to harass and silence investigative journalists and public interest defenders.<sup>xxv</sup> In particular, they asked the EU to:

- Adopt an Anti-SLAPP Directive, which would introduce exemplary sanctions to be applied to claimants bringing abusive lawsuits, procedural safeguards for SLAPP victims, and other preventive measures.
- Reform the Brussels I Regulation with a view to modify rules which allow claimants to choose where to make a claim, to end “forum shopping” in defamation cases as well as imposing excessive expenses on defendants who are forced to hire and pay for lawyers in countries where they are not based.
- Reform the Rome II Regulation so that it regulates which national law applies to a defamation case to prevent claimants from selecting legal regime where laws that are restrictive of freedom of expression might favor their case.
- Support victims of SLAPPs by allocating funds, especially to ensure legal defense and train judges and practitioners.
- Create a public EU register of companies that engage repetitively in SLAPPs.

In response to concern about SLAPPs, the European Commission announced, in its Work Programme for 2021, action to protect journalists and civil society against strategic lawsuits against public participation in the form of an initiative against abusive litigation targeting journalists and civil society (legislative or non-legislative), in the last quarter of 2021.

As for the situation of **journalists**, press freedom is a fundamental right established in the EU Charter of Fundamental Rights. Nevertheless, there are no specific legal frameworks at the European Union level protecting journalists from retaliation for investigating and reporting on corporate misconduct. The EU, in 2014, has adopted a set of Human Rights Guidelines on Freedom of Expression Online and Offline (2014) that places an onus on the EU to call on all States to take active steps to prevent violence against journalists and other media actors, enabling them to work in safety and security, without fear of violence and persecution. It is also envisioned that the forthcoming work to propose protection against SLAPPs would expressly address retaliation in the form of lawsuits against journalists. The Guidelines also provide political and operational guidance to officials and staff of the EU Institutions and EU Member States for their work in third countries and in multilateral fora as well as in contacts with international organisations, civil society and other stakeholders.

*While targeted action by the EU to counter SLAPPs against NGOs and journalists could serve to address risks of retaliation for reporting corporate misconduct including in global supply chains, it would address only one form of risk of retaliation that these categories currently face, rather than the full spectrum of risks.*

Through broad and encompassing guidelines, the EU has also issued support for **human rights defenders** – which many of those reporting on corporate misconduct under the proposed Directive could be considered as should they so wish. This support is principally manifested in a set of Guidelines establishing the practical steps that the EU will take to protect such individuals.<sup>xxvi</sup> The EU's Human Rights Defender Guidelines have particularly been used to support individuals that identify as human rights defenders and that live and work in non-EU member states. Specifically, the EU Human Rights Defender Guidelines advise that EU actions should include the following:

- EU missions should be encouraged to adopt a pro-active approach towards human rights defenders. This includes establishing contacts with defenders, receiving them in the mission premises, visiting them on the ground, and increasing their public recognition through the media or through invitations and visits. EU missions should also send observers to trials of defenders and visit defenders in custody.
- The EU should issue démarches and/or public statements through for example, the EU delegation based in the relevant country, the EU High Representative, the EU Special Representative for Human Rights or the EEAS spokesperson. Cases of human rights defenders in peril should be raised during political or human rights dialogues with the countries concerned or during high-level visits. When visiting a country, high-ranking EU officials should include meetings with human rights defenders in their programmes.
- EU delegations are expected to report periodically on the situation of human rights defenders. They should organize an annual meeting between defenders and EU diplomats in order to coordinate and share relevant information.
- Heads of delegations should make recommendations to the Council of the EU's Working Party on Human Rights (COHOM) for possible EU action, especially concerning defenders at immediate risk.
- As an overarching objective, the EU should encourage third countries to create an environment in which human rights defenders can operate freely.

To better address the urgent need for protection of defenders facing imminent risks but also to provide them with longer-term assistance, including shelter, a comprehensive EU-funded mechanism

(protectdefenders.eu) was also established in October 2015 and is currently being implemented by a consortium of human rights organizations. This protection mechanism has supported a number of communities and individuals that have been threatened by companies, including by companies based in the EU.

*The EU's Human Rights Defenders Guidelines and associated protection mechanism is principally relevant for individuals and groups that wish to be referred to as human rights defenders and that have already been subject to harm. However, it seems less relevant as a preventative mechanism and it does not impose any particular requirements on companies or member states to protect against retaliation. In addition, while the term human rights defenders is typically used in an all-encompassing way to refer to any individuals and groups that in peaceful manners work to promote human rights, some individuals, communities and organizations may not, for a number of reasons, wish to rely on this term. In short, it is unclear to what extent this term is functionable for addressing retaliation by companies against a broad group of stakeholders that may suffer harm, including employees, whistle-blowers, local communities, NGOs, lawyers, journalists, complainants to independent accountability mechanisms or others supporting the work of such mechanisms, such as drivers, interpreters and local facilitators. One of the central arguments of this submission is that individuals and groups should be afforded protection against reprisals for reporting corporate misconduct, or for seeking to engage with companies over risks and impacts, without having to defer the term human rights defender. Protection should also be connected to legal Directives, rather than by single references to policy documents that do not have legal bearing on neither Member states nor companies.*

## How have risks of retaliation been reflected to date in due diligence initiatives?

### Due diligence initiatives at the national level

The proposal for a new EU Directive on mandatory human rights due diligence follows suit a number of national legal and policy developments that require companies to conduct human rights due diligence or to report on the measures, if any, that they have taken to address risks in their supply chains. For example, countries like the US, France, the UK and the Netherlands have adopted specific due diligence requirements – addressing all supply chain risks or specifically focusing on some – for companies under their jurisdiction. In Switzerland, Germany and Norway, similar initiatives are likely to be adopted.

In some of these initiatives, risks of retaliation against individuals or groups that report on companies' non-compliance are specifically included, at times also extending beyond the employer-employee context. For example:

The **US Dodd-Frank Act (2010)** – which includes a requirement for companies to disclose their use of tin, tungsten, tantalum and gold in their products and to determine if these minerals have been sourced responsibly – establishes a whistle-blower protection program that requires the US Securities and Exchange Commission (SEC) to pay an award to eligible whistle-blowers who voluntarily provide the Commission with original information about a violation of the federal securities laws that leads to the successful enforcement of a covered judicial or administrative action, or a related action. The Dodd-Frank Act also prohibits retaliation by employers against individuals who provide the SEC with information about possible securities violations. In addition to protecting whistle-blowers who have reported possible securities law violations from retaliation, an additional SEC Rule<sup>xxvii</sup> prohibits any person from taking any action with the view to prevent someone from contacting the SEC directly to report a possible securities law violation. The Rule states that “[n]o person may take action to impede an individual from communicating directly with the Commission staff about a possible securities law violation, including enforcing, or threatening to enforce, a confidentiality agreement...with respect to such communications.” Unlike the anti-retaliation protections of the Act, the protections against actions taken to impede reporting possible securities law violations are not limited to the employee-employer context. Only the SEC, however, may file an enforcement action for a violation of this rule. The Dodd-Frank does not specifically state whether, or to what extent, the anti-retaliation protections apply to individuals or conduct outside of the United States, but the SEC has confirmed that whistle-blowers do not need to reside or work in the United States to be eligible for an award under the Commission’s whistle-blower award program.<sup>xxviii</sup>

Also in the US, the **Federal Acquisition Regulation governing public procurement by US Federal Agencies (1984)** prohibits the use of forced or indentured child labour and the reliance on human trafficking for federal contracts performed outside the US. The Government will also not provide contracts to any company that has not certified that it will not sell a product that is suspected of having been produced with forced or indentured child labour.<sup>xxix</sup> The Federal Acquisition Regulation was further strengthened in 2015 to require federal government agencies to impose contractual obligations on any sub-contractors to prevent human trafficking and forced labour. With the amendment, contractors are required to prepare certification and compliance plans for contracts performed outside of the US and exceeding USD 500 000.<sup>xxx</sup> Under the regulation, these companies must satisfy certain additional requirements, including maintaining a process for employees to report, *without fear of retaliation*, activity inconsistent with the policy.<sup>xxxi</sup>

**France's 'Loi relative au devoir de vigilance des sociétés mères et des entreprises donneuses d'ordre'** (2017) requires companies with at least 5,000 employees in France or 10,000 worldwide to conduct due diligence across their own operations and supply chains. This due diligence should result in a vigilance plan addressing the relevant risks and how these have been managed or will be managed. The Law provides three judicial mechanisms to ensure effective implementation of the duty of vigilance: a formal notice to comply, an injunction with periodic penalty payments, and a civil liability action in case of a damage. These mechanisms are available to any party with standing, which includes stakeholders whose rights could be affected by a company's operations and activities, for example local communities, employees, trade unions, associations or NGOs. Risks of retaliation are not expressly referred to in the law. While the law does not expressly refer to risks of retaliation or imposes any obligations on companies to ensure safe stakeholder engagement, emerging practice in France is worthy of note. The **Anti-Corruption Sapin II Law (2016)** brought French legislation in line with the most exacting European and international standards by creating a dedicated French Anti-Corruption agency, *Agence Française Anti-Corruption* (AFA), that can impose sanctions in case of any identified breaches. The Sapin II Law is principally preventive in nature and stipulates that companies must establish an anti-corruption program to identify and mitigate corruption risks. It has an extraterritorial scope and establishes protection against retaliation for whistle-blowers. In many respects, the requirements of Sapin II and the Loi relative au devoir de vigilance des sociétés mères et des entreprises donneuses d'ordre overlap: both require companies to conduct a risk mapping to identify, analyze and prioritize risks, procedures to evaluate third parties, system of alerts, and a monitoring scheme. Because of this, a number of French companies have started to create cross-functional working groups to implement the requirements of both laws, including by strengthening whistle-blowing systems. This has entailed combining existing confidential grievance mechanisms and hotlines to identify corruption and human rights issues simultaneously. Some companies have established mechanisms of this kind that are available to third parties and run by external third parties to protect anonymity.<sup>xxxii</sup>

The **Dutch Child Labour Law** (2019) requires companies to engage in due diligence regarding child labour in the supply chain and to disclose these activities. Implementation of the law is supervised by a regulatory authority (Toezichthouder) that will publish all reports. This authority has the power to impose administrative fines for non-compliance. Any natural person or legal entity whose interests are affected by the actions or omissions of a company relating to the law has the right to submit a complaint to the regulatory authority after having first attempted to resolve the complaint directly with the company, or six months after the submission of the complaint to the company without it having been addressed. There is no publicly available information to suggest that risks of reprisals against complainants enjoy particular protection against reprisals in this regard. Also in the Netherlands, the **Dutch Agreements on International Responsible Business Conduct** – where signatory companies in different sectors work with the government, trade unions and NGOs to develop long-term strategies to tackle complex problems in their global supply chains – make sparse references to risks of retaliation. These references are principally to be found in the terms of references for the Sector Covenants' complaints mechanisms and principally establish procedural safeguards such as the right of complaints to have their personal identity protected where needed.

The **UK's Modern Slavery Act** (2015) requires companies with a global turnover of more than £36 million to make an annual statement on their activities to address forced labour and trafficking in their own operations and supply chains. To monitor compliance with the Act, the UK Government relies on the scrutiny of civil society. There are no specific provisions to ensure that civil society actors are protected from acts of retaliation for raising concerns over companies' lack of reporting, or poor-quality reporting, under the Act. Similarly, the **Australia Modern Slavery Act** (2018) establishes

reporting obligations on Australian companies that meet an annual consolidated revenue of \$100 million or more. Companies are expected to report on the risk of modern slavery in the operations and supply chain (and risks associated with its owned and controlled entities), and on the steps it has taken to respond to the risks that have been identified. Unlike other jurisdictions, the reporting criteria in Australia are mandatory. The Australian Government publishes these statements through an online publicly accessible register, which is operational as of July 2020. There is no specific reference to retaliation risks of how to address these, neither in the context of company reporting requirement, nor in terms of raising instances of non-compliance with the Act in Australia.

## **EU-adopted supply chain due diligence initiatives**

In other EU directives and associated guidance on mandatory due diligence for companies, risks of retaliation appear to be largely neglected. For example:

**Directive 2014/95/EU, amending Directive 2013/34/EU as regards disclosure of non-financial and diversity information by certain large undertakings and groups** (2014), refers to Member States' obligation to "ensure that adequate and effective means exist to guarantee disclosure of non-financial information by undertakings in compliance with this Directive. To that end, Member States should ensure that effective national procedures are in place to enforce compliance with the obligations laid down by this Directive, and that those procedures are available to all persons and legal entities having a legitimate interest, in accordance with national law, in ensuring that the provisions of this Directive are respected. The Directive does not, however, specifically refer to the risks that stakeholders are likely to face for seeking information or expressing concern over companies' environmental and social risks management or lack thereof.

**Regulation 2017/821 concerning supply chain due diligence obligations for Union importers of tin, tantalum and tungsten and gold originating from conflict-affected and high-risk areas (the Conflict Minerals Regulation)** (2017) remains silent on risks of retaliation against those that report on Union economic operators' non-compliance with the Directive, despite the fact that the OECD's Guidance on Conflict Minerals – which serves as the point of reference and baseline measure of the Directive specifically refers to security concerns – including to whistle-blowers – in the context of reporting on due diligence.<sup>xxxiii</sup>

Similarly, **Regulation 995/2010 on obligations of operators who place timber and timber products on the market (the Timber Regulation)** (2010) and its associated guidance does not make any reference to the safety of those that may report companies' non-compliance with the regulation and the risks to their personal security for doing so.

## How are risks of retaliation reflected in current discussions over the proposed directive?

The need to address risks of retaliation has been highlighted in the background briefing requested by the European Parliament to inform the debates about the scope and content of the Directive. It noted that victims of corporate misconduct continue to face legal and practical obstacles to access to justice and effective remedy, including attacks on human rights defenders, victims, witnesses, lawyers, judges and journalists and the risk of counter-litigation, including SLAPPs.<sup>xxxiv</sup> The briefing emphasized that any proposed legislation should help protect human rights defenders,<sup>xxxv</sup> and suggested that further analysis is necessary to ensure the appropriate arrangements for stakeholders – including human rights defenders and trade unionists – to be able to monitor companies' compliance with the directive.<sup>xxxvi</sup> The briefing also calls on the EU to continue to cooperate with member states towards removing legal and other threats to human rights defenders, civil society organisations and other actors or participants in the justice system *inter alia* via SLAPP suits.<sup>xxxvii</sup>

While the power to propose the Directive rests with the European Commission, a report in the form of a draft Directive was presented by Member of European Parliament Lara Wolters and the European Parliament's Committee on Legal Affairs in September 2020. The 'Wolter report' reflects risks of retaliation in a number of ways. For example, the motion for a European Parliament resolution notes that:

- To avoid the risk of critical stakeholder voices remaining unheard or marginalised in the due diligence process, the Directive grants stakeholders the right to safe and meaningful consultation as regards the company's due diligence strategy, and ensure the appropriate involvement of trade unions (paragraph 28).
- Complaint procedures should ensure that the anonymity, safety, physical and legal integrity of whistle-blowers is protected, in line with Directive (EU) 2019/1937 of the European Parliament and of the Council (paragraph 29).

The annex to the motion for a resolution (recommendations on content of the directive) establishes that:

- Effective *protection mechanisms and measures* should be put in place by the undertaking to ensure that affected or potentially affected stakeholders are not put at risk due to participating in the consultations that are undertaken as part of a company's due diligence (Article 5.3, emphasis added).
- Workers or their representatives should be informed and consulted on the due diligence strategy of their undertaking in accordance with Directive 2002/14/EC establishing a general framework for informing and consulting employees in the European Community,<sup>xxxviii</sup> Directive 2009/38/EC on the establishment of a European Works Council<sup>xxxix</sup> and Council Directive 2001/86/EC supplementing the Statute for a European undertaking with regard to the involvement of employees<sup>xl</sup> (Article 5.5). These Directives contain important references to zero-tolerance against retaliation against workers participating, in their capacity as trade unionists or worker representatives or otherwise, in company-led consultations.
- Grievance mechanisms should be legitimate, accessible, predictable, *safe*, equitable, transparent, rights-compatible and adaptable as set out in the effectiveness criteria for nonjudicial grievance mechanisms in Principle 31 of the United Nations Guiding Principles on Business and Human Rights. They should provide for anonymous complaints. (Article 9.2, emphasis added).

- Member States should facilitate the submission by third parties of complaints ... by measures such as complaint submission forms and ensuring that complaints *remain anonymous upon the request of the complainant* (Article 15.3, emphasis added).

In short, the proposed text places a positive obligation on companies to ensure safe consultations with stakeholders. It also requires companies to ensure the safe access of stakeholders to grievance mechanisms, with reference to the EU's Whistleblower Protection Directive. The references to Directives establishing the obligation for EU-based companies to inform and consult workers on matters that may have an impact on their rights also, albeit indirectly, imply the protection against retaliation for employees within the EU while acting as worker representatives for the purpose of the Directive.

Nevertheless, the proposal:

- Does not clearly recognize that individuals and groups that express concern over companies' operations and business relationship can be subject to retaliation for doing so.
- Does not refer to the fact that under the international bill of human rights, companies should at all times respect the right of stakeholders to freely express their views.
- Does not place a clear negative obligation on companies to not retaliate against stakeholders that have engaged with them and express diverging views, or that decide to publicly voice concerns – in the media, before courts of law, through public advocacy campaigns or by other means – over the risks and impacts associated to their direct operations, supply chains and business relationships.
- Does not require companies to communicate to their business relationships a zero-tolerance approach to retaliation against stakeholders.
- Does not require companies to consider risks of retaliation that they can cause, contribute to or be directly linked with through the operations, products and services
- Does not define what safe stakeholder engagement or safe access to complaints mechanisms is and could look like in practice, or make reference to any forthcoming guidance in this regard.
- Makes reference to the EU's Whistleblower protection directive in an all-encompassing way despite the fact that companies/member states are not, per se, required to ensure protection against retaliation for reporting on supply chain risks and impacts or to extend this protection to the groups that are most at risk (local communities, local activists, NGOs). In this regard, the recommendations do not suggest that Member States should transpose the Whistleblower protection mechanism to cover all areas of national law to ensure that its protective scope also applies to those reporting on companies non-compliance with the directive on mandatory human rights due diligence.
- Does not refer specifically to the need for designated competent authorities to take into account risks of retaliation against stakeholders who seek information about, or report on misconduct of, companies within their jurisdiction, aside from providing for the possibility to grant complainants to the authorities anonymity if they so wish.
- Recommends amendments to existing European regulations dealing with jurisdiction and recognition of judgments and governing law for non-contractual obligations (the 'Brussels Recast Regulation' and the 'Rome II Regulation'). If adopted, this would, on the one hand, render it easier to bring claims against EU-domiciled parent companies for harms caused by their non-EU subsidiaries or an undertaking with which they have a business relationship, make it possible for EU Member State courts to take jurisdiction on an exceptional basis over matters occurring in third countries where there is inadequate access to justice and allow



victims of business-related human rights abuses committed within the value chains of EU undertakings to choose for non-contractual claims to be governed by a law with high human rights standards (including the law of the country of domicile of the parent company of the undertaking). In short, it would facilitate access to remedy by allowing for lawsuits to be brought against EU-based undertakings which could also increase risks of retaliation against victims or their representatives if not coupled with specific safeguards to this end. In this regard, the proposal to reform the 'Brussels Recast Regulation' and the 'Rome II Regulation' does not refer to any amendments to allow claimants to choose where to make a claim, to end "forum shopping" in defamation cases as well as imposing excessive expenses on defendants who are forced to hire and pay for lawyers in countries where they are not based, or to reform the Rome II Regulation so that it regulates which national law applies to a defamation case to prevent claimants from selecting legal regime where laws that are restrictive of freedom of expression might favor their case.

## How to reflect risks of retaliation in a coherent manner in the Directive: practical suggestions and recommendations

The concluding part of this submission puts forward practical recommendations for how the EU, through the mandatory human rights due diligence directive and any implementing guidance to companies and member states, could reflect risks of retaliation.

Recommendations are based on the five-step due diligence framework of the OECD and have been grouped according to three principal areas:

- What can the EU ask companies to do?
- What can the EU do to reduce risks of reprisals and to respond to retaliation that has occurred ?
- What can the EU ask Member States to do when transposing the Directive?

### 1. What can the EU ask companies to do?

**What can the EU, through its Directive and associated procedural guidance, ask companies to do? More specifically, how can the Commission place a negative obligation on companies to not retaliate against stakeholders? How can the Commission encourage companies' to take appropriate steps to identify, prevent, cease, mitigate and monitor risks of retaliation against a broad range of stakeholders, account for how these have been managed (with due regard for any concerns to personal safety) and remediate instances of retaliation that have occurred?**

**Pro-actively communicating zero-tolerance to retaliation to companies is one of the most – if not the most – effective measure to prevent retaliation.** At a minimum, the Directive itself should recognize that stakeholders, including local communities, individuals and organisations working to expose business-related environmental, human rights and governance risks and harms, trade unionists and worker representatives – are important sources of information for companies' due diligence processes, and that companies should respect their right to freely express their opinions and views – including critical – at all times. It should recognize that the individuals, communities and organisations that raise concerns or otherwise address risks and impacts associated with companies' operations and activities, or those of their business relationships – can face genuine risks of retaliation for doing so, and place **a negative obligation on companies to not take acts in reprisals or sanction acts of reprisals taken by business relationships**. The Directive should define reprisals as any detrimental action that impairs or harms, or threatens to impair or harm, anyone seeking to, or having, expressed opinions, concerns, or opposition to a company's activities or to the activities of its relevant business relationships, and that the types of acts that the umbrella term retaliation covers can include, but are not limited to any, or a combination of, intimidation and threats, slander and defamation, strategic lawsuits against public participation, electronic or physical surveillance, property damage or loss, physical attacks leading to bodily harm or fatality, or discrimination, disadvantage or adverse treatment in relation to employment.

The Directive should also place a **positive obligation on companies to prevent retaliation. This would entail that companies should, as part of their due diligence, be required to seek to ensure that all stakeholders – including those with critical views – can express their views in a manner that does not cause them, or others associated with them, any harm.** More specifically, as part of their due diligence and enabling access to remedy, companies should be expected to identify, assess and prioritize risks of retaliation against stakeholders and to put in place any measures needed to prevent, mitigate or otherwise address these risks depending on their level of involvement (cause, contribute

to, directly linked to), in collaboration with those concerned. This can include, amongst other, proactively including references to zero-tolerance to retaliation in commercial contracts with business partners and requesting that these requirements be cascaded down to the next part in the supply chain and otherwise communicating this expectation to business relationships including State authorities, ensuring safe channels for those at risk to communicate any concerns they have about their safety, and enabling victims of retaliation to seek remedy to restore them to their original situation had harmed (retaliation) not occurred.

If liability is reflected in the Directive, this submission recommends that **criminal liability – corporate and individual – should be an option in cases where companies have been found to have caused or can reasonably, in all the circumstances of the situation at hand, be considered to have contributed to severe forms of retaliation (such as, for example, bodily harm or fatalities)**. National legislative frameworks on corruption – notably the UK Bribery Act (2010) – can provide a useful model in this regard (liability for the failure to prevent, coupled with the defence of having put in place adequate prevention procedures). More specifically, in terms of severe forms of retaliation, it is recommended that **criminal liability be linked to companies' failure to prevent retaliation by associated persons to impair or harm anyone seeking to, or having, expressed opinions, concerns, or opposition to a company's activities or to the activities of its business relationships.**<sup>xli</sup> To ensure that remedy for those that have suffered the retaliation is not out of reach, a provision on civil remedy for damages should also be reflected in the Directive.

With the understanding that the Directive itself will not provide particular guidance on thematic risks that can have an impact on, or be particularly relevant for, companies' due diligence processes, the **Directive could refer to forthcoming implementation guidance** for companies and Member States and note that **safe stakeholder engagement in general, and risks of retaliation in particular, will be further elaborated in these with actionable examples.**

**2. Should the Commission, in the legislative proposal and/or associated procedural guidance, tie any specific references to retaliation to relevant directives and policies at the EU level?**

The current protections afforded by EU Directives to the different groups that are typically subject to reprisals for addressing corporate misconduct currently form a haphazard and uneven patchwork, and it is unclear to what extent existing directives could be relied on to prevent retaliation or to address retaliation that has occurred. **Should the Commission choose to refer to Directives like the Whistleblower protection directive, it should be made clear at the outset that additional measures should be taken by both companies and member states to prevent, mitigate and respond to risks of retaliation and address instances of retaliation that have occurred against a broader group of stakeholders than those that could potentially enjoy a certain degree of protection under the Whistleblower protection directive for reporting corporate misconduct.** More broadly, the European Commission's ongoing work to develop a legislative or non-legislative initiative on action to protect journalists and civil society against strategic lawsuits against public participation in the last quarter of 2021 remains particularly important and **could be cross-referenced in the directive on mandatory human rights due diligence and in any associated guidance.**

**3. What can the EU do to reduce risks of reprisals and to respond to retaliation that has occurred ?**

The European Commission's ongoing work to develop a **legislative or non-legislative initiative on action to protect journalists and civil society against SLAPPs** also remains particularly important to prevent instances of retaliation in the form of SLAPPs within the EU. In this regard, a **proposal for an anti-SLAPP Directive should recommend reforms to the 'Brussels Recast Regulation'** to allow

claimants to choose where to make a claim, to end “forum shopping” in defamation cases as well as imposing excessive expenses on defendants who are forced to hire and pay for lawyers in countries where they are not based, and **to the Rome II Regulation** so that it regulates which national law applies to a defamation case to prevent claimants from selecting legal regime where laws that are restrictive of freedom of expression might favour their case.

In addition, the Commission is advised to initiating work to develop **legislative or non-legislative initiatives to expand current source protection (source confidentiality)** – the right accorded to journalists under international law and certain national legal frameworks to not disclose the identity of their sources – **to also include other professionals, in particular non-governmental organizations, to be able to invoke the right to source protection when bringing business and human rights claims against companies in front of national courts of law.** Without a strong guarantee of anonymity, many NGOs that are working to bring complaints have decided not to do so because courts have been unable, or unwilling, to expand this protection to the original claimants or to those that have provided crucial information needed to initiate proceedings.

#### **4. What can the EU ask Member States to do?**

**With regards to Member States’ enforcement of the Directive on mandatory due diligence through the transposition into national law, the Directive should include particular consideration of, and reference to, risks of retaliation and how these will be managed by Member States, including by any designated authorities that will oversee the enforcement of the Directive.** Addressing risks of retaliation should entail going beyond simply granting potential complainants the right to remain anonymous.<sup>xlii</sup> In particular, identifying and managing risks of retaliation should be considered, and cross-referenced for the following:

- In terms of any effective, proportionate and dissuasive penalties, including civil and criminal, that the directive will propose, as has been noted, this submission recommends that **criminal liability – corporate and individual – should be an option in cases where companies have been found to have caused, or can reasonably, in all the circumstances of the situation at hand, be considered to have contributed to, severe forms of retaliation (such as, for example, bodily harm or fatalities) against stakeholders that have voiced concerns over their activities or those of their business partners and been subject to harm because of that.** National legislative frameworks on corruption – notably the UK Bribery Act (2010) – can provide a useful model in this regard (liability for the failure to prevent, coupled with the defence of having put in place adequate prevention procedures). In terms of severe forms of retaliation, it is recommended that **liability be linked to companies’ failure to prevent retaliation by associated persons to impair or harm anyone seeking to, or having, expressed opinions, concerns, or opposition to a company’s activities or to the activities of its business relationships.**<sup>xliii</sup> The complex question of responsibility for retaliatory actions of companies’ business relationships in their supply chain should be determined by a court, with reference to reasonableness of the due diligence undertaken, including leverage exercised in the relevant circumstances. **To ensure that remedy for those that have suffered the retaliation is not out of reach, a provision on civil remedy for damages should also be reflected in the Directive. As such, having suffered retaliation should in itself be sufficient grounds for victims to bring cases in front of national courts of law.**
- Where **instances of retaliation have been reported**, and in line with established practice in the field of whistle-blower protection, Member States should establish that the **burden of proof falls on the company**, not on the individual or group that claim to have been

subject to retaliation. In other words, where companies are alleged to have caused or contributed to retaliation, companies should be requested to present evidence to the contrary, and that adequate prevention has been put in place to reduce risks of retaliation, through the conduct of appropriate due diligence that is proportionate to the identified level of risk.

- When establishing enforcement rights and procedures for interested parties, the **designated authority or authorities** that may supervise the proper enforcement of the Directive should **have dedicated policies on how to protect individuals (complainants or others) from retaliation for submitting complaints or otherwise engaging with companies to express concerns over risks or impacts that they have caused, contributed to or been directly linked to**. Such policies should go beyond merely granting the right to anonymity of complainants, and should include proactive risk assessments and the development of risk mitigation measures, in consultation with those concerned.
- If providing **competent bodies the right to investigate abuses, initiate enforcement actions and support victims**, appropriate procedures should be developed to identify and effectively manage risks of retaliation, in close consultation with those concerned. This requires that staff of the competent bodies have the **right set of skills and protocols in place and the possibility to collaborate with other actors, including in a cross-border context, to mitigate and address risks. As appropriate, competent bodies should have within their “toolbox” the option to also take steps to protect persons at risk in countries outside the EU**, such as by working with police teams in the countries concerned, where victims have agreed to doing so and would not expose them to further risks.
- When facilitating and providing effective means of remedy for victims (including judicial and non-judicial remedies), member states should **encourage companies to put in place appropriate grievance mechanisms that can be accessed by potential complainants without exposing them to risks of retaliation**, including by, for example accepting anonymous submissions, or by collaborating with other actors, such as, for example, independent national human rights institutions, to accept complaints linked to their activities or business relationships in challenging contexts. Companies should be encouraged to **assess to what extent the grievance mechanisms run by multi-stakeholder initiatives in which they participate can ensure safe access and the safe handling of complaints** for complainants and others associated with them or the complaints handling process. At the **national level, grievance mechanisms – including for example National Contact Points – should also be strengthened to ensure safe access**. In **liability claims, retaliation should in itself constitute sufficient grounds for lawsuits. Where retaliation is found to have taken place, Member States should consider granting victims within the EU access to national criminal compensation schemes to help repair the harm that they have suffered**.

## References

<sup>i</sup> Section 7 of the UK Anti-Bribery Act (2010) took a new approach to corporate criminal liability by making companies criminally liable for failing to prevent bribery by associated persons (subject to a compliance defense of having 'adequate' anti-bribery procedures in place).

<sup>ii</sup> Remaining anonymous is one potential strategy to address risks of retaliation, and often the default option to protect individuals and organisations from being exposed to harm. Nevertheless, depending on the context and the preferences of those at risk, other strategies may be a better option to prevent or mitigate risks, including, for example issuing public statements recognizing their right to express freely their opinion or communicating clearly to the companies concerned, at the outset of a complaints handling process, investigation or other procedure that retaliation will not be tolerated.

<sup>iii</sup> Section 7 of the UK Anti-Bribery Act (2010) took a new approach to corporate criminal liability by making companies criminally liable for failing to prevent bribery by associated persons (subject to a compliance defense of having 'adequate' anti-bribery procedures in place).

<sup>iv</sup> This paper uses the terms retaliation and reprisal interchangeably. Broadly, retaliation/reprisal is an umbrella term that refers to any detrimental action that impairs or harms, or threatens to impair or harm, anyone seeking to, or having, expressed opinions, concerns, or opposition to a company's activities or to the activities of its business relationships. The types of acts that this term covers can include, but are not limited to any, or a combination of, the following: verbal intimidation and threats, slander and defamation, strategic lawsuits against public participation, electronic or physical surveillance, property damage or loss, restrictions to freedom of movement, travel bans, physical attacks leading to bodily harm or fatality, discrimination, disadvantage or adverse treatment in relation to employment.

<sup>v</sup> While more reports of retaliation are surfacing – in part due to the establishment of dedicated channels for providing such information – their real extent is likely to be much higher. Numbers are underreported due to a lack of awareness of those impacted of channels available for reporting incidents, or out of fear of being subject to further retaliation if reports become public. Where information is available, it typically focuses on the most serious forms of retaliation, such as legal harassment or physical violence, and less so on other more subtle forms, such as, for example, defamation and slander or loss of employment-related opportunities. These limitations to data make it challenging to estimate whether there is a higher likelihood of retaliation in some regions or sectors, or whether certain groups face higher risks or are more impacted than others. Nevertheless, an analysis of the work done by individuals that were killed in 2019 is instructive: of the total reported number of 300 deaths, 40 % were engaged in advocacy related to land, environmental and indigenous peoples' rights. As such, sectors with a large physical footprint – agribusiness, energy and transport in particular – appear to come with higher-risks than others. Most of the recorded attacks took place in Latin America, followed by Asia and the Pacific region, and Eastern Europe and Russia (Business and Human Rights Resource Centre, Human Rights Defenders and Business. January 2020 Snapshot).

<sup>vi</sup> CIVICUS Civic Space Monitor, 2019.

<sup>vii</sup> See for example, statement on Egypt ([https://eeas.europa.eu/headquarters/headquarters-homepage/89101/egypt-statement-spokesperson-recent-arrests-human-rights-activists\\_en](https://eeas.europa.eu/headquarters/headquarters-homepage/89101/egypt-statement-spokesperson-recent-arrests-human-rights-activists_en)),

<sup>viii</sup> [https://www.europarl.europa.eu/RegData/etudes/BRIE/2018/630267/EPRS\\_BRI\(2018\)630267\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2018/630267/EPRS_BRI(2018)630267_EN.pdf)

<sup>ix</sup> See, for example, sanctions imposed on Burundi (10/2015), China (06/1989), Guinea (10/2020), Iran (04/2020), Venezuela (11/2020) and Zimbabwe (02/2020).

<sup>x</sup> Council of the European Union, Conclusions on EU Priorities in UN Human Rights Fora in 2020, Brussels, 17 February 2020.

<sup>xi</sup> Study on Due Diligence requirements throughout the supply chain, January 2020. Prepared by British Institute of International and Comparative Law (lead), Civic Consulting and LSE Consulting for the European Commission Directorate-General for Justice and Consumers Directorate. Footnote 813. For the database on attacks, see at <https://www.business-humanrights.org/en/big-issues/human-rights-defenders-civic-freedoms/>

<sup>xii</sup> EU Human Rights Due Diligence Legislation: Monitoring, Enforcement and Access to Justice for Victims (Briefing requested by the DROI Subcommittee (June 2020), p. 1.

<sup>xiii</sup> Such factors include, for example, laws, practice or other circumstances at the country level that restrict peoples' ability to engage freely in public debates and/or deter people from expressing their views.

<sup>xiv</sup> The following examples can be useful to consider when evaluating level of involvement with retaliation (adapted from OECD, 2018. Due Diligence Guidance for Responsible Business Conduct):

A company **causes** the retaliation if its activities, on their own, suffice to result in the adverse impact. For example: a company instigating a strategic lawsuit against public participation against an NGO that has sought to expose impacts in its supply chain would be causing the adverse impact (retaliation).

A company **contributes to** retaliation if its activities, in combination with activities of other entities, cause the impact, or if the activities of the company cause, incentivize or facilitate another entity to retaliate.

Determining whether a company has contributed to retaliation includes considering the following issues.

- The extent to which the company may encourage or motivate retaliation by another entity, i.e. the degree to which the activity increased the risk of the retaliation occurring.
- The extent to which a company could or should have known about the retaliation of potential for retaliation, i.e. the degree of foreseeability.
- The degree to which any of the company's activities actually mitigated the retaliation or decreased the risk of it occurring.

For example, a company engages public security forces to protect its project area, equipment and personnel in an area where local tensions around the project run high. In the past, public security forces in the area have resorted to the disproportionate use of violence against community leaders in the context of peaceful demonstrations against the project at the site and information publicly available information suggests that government authorities have started targeting community leaders and mobilized a campaign against them on social media. There are no contractual arrangements to ensure that public security forces have received the adequate training to respond to demonstrations.

A company is **directly linked** to retaliation where there is a link between the retaliation and the company's products, services or operations by another entity (i.e. business relationship). For example, a company is sourcing cotton from a country where the use of forced labour and child labour is prevalent. Local organisations and activists that have sought to raise attention to working conditions have been subject to attacks orchestrated by local government authorities and companies. In this situation, the company is not causing or contributing to retaliation, but it is directly linked to it because there is a direct link between its products and retaliation through its business relationships with the entities involved in producing and sourcing of the cotton.

<sup>xv</sup> These examples are based on publicly available information, including media articles, reports from international and regional human rights mechanisms and court decisions, but also interviews with local activists and the experience of the author herself from having worked to identify and manage risks of, and de facto, retaliation.

<sup>xvi</sup> According to available data from the EU, fear of suffering retaliation has a chilling effect on potential whistleblowers. Answering to the 2017 Special Eurobarometer on corruption, 81% of respondents said that they did not report the corruption that they had experienced or witnessed. Similarly, 85% of respondents to the Commission's 2017 public consultation expressed the view that workers very rarely or rarely report concerns about threat or harm to the public interest. Fear of legal and financial consequences was the reason most widely cited for that why workers do not report wrongdoing. See [https://ec.europa.eu/info/sites/info/files/placeholder\\_11.pdf](https://ec.europa.eu/info/sites/info/files/placeholder_11.pdf).

<sup>xvii</sup> In response to the increase in reports of retaliation against stakeholders, a number of companies have adopted policies and codes of conduct addressing these risks. For example, a number of development finance institutions – multilateral and bilateral – have released public-facing documents on how retaliation will be addressed (cf. [IFC position statement](#) (2018)). Beyond the development finance context, a number of multinational companies have also taken the lead to address retaliation against their stakeholder, including through zero-tolerance position statements on retaliation against stakeholders, also those critical of the companies' activities (see, for example [ENI](#), [Vale](#) and [Kelloggs](#)) or through a narrower focus on workers by including dedicated provisions against retaliation against workers in supplier codes of conduct and enforcement protocols (see, for example, [ADIDAS](#)).

<sup>xviii</sup> In addition to the Directive itself, the following sections draw on the article 'The European Union Whistleblower Directive: A 'Game Changer' for Whistleblowing Protection?' by Vigjilence Abazi, published in the *Industrial Law Journal*, Volume 49, Issue 4, December 2020, Pages 640–656, <https://doi.org/10.1093/indlaw/dwaa023>

<sup>xix</sup> Directive 2002/14/EC establishing a general framework for informing and consulting employees in the European Community, Article 7.

<sup>xx</sup> Directive 2009/38/EC on the establishment of a European Works Council, Article 34.

<sup>xxi</sup> Council Directive 2001/86/EC supplementing the Statute for a European undertaking with regard to the involvement of employees, Article 10.

- 
- <sup>xxii</sup> European Union Agency for Fundamental Rights (FRA), 2020. Business and Human Rights: Access to Remedy, pg. 10.
- <sup>xxiii</sup> Bárd P., Bayer J., Chun Luk, N., Vosyliute L. for the Academic Network on European Citizenship Rights: Ad Hoc Request – SLAPPs in the EU context. May 2020, pg. 17.
- <sup>xxiv</sup> Ibid.
- <sup>xxv</sup> Ending Gag-Lawsuits in Europe: Protecting Democracy and Fundamental Rights, June 2020. Available at <https://www.access-info.org/wp-content/uploads/2020-06-05-Ending-SLAPPs-NGO-Policy-Paper-119-FINAL.pdf>
- <sup>xxvi</sup> The following section draw on the European Union’s Human Rights Defenders Policy, and an associated European Parliament Briefing on the implementation of this Policy, issued in 2018 and available at [https://www.europarl.europa.eu/RegData/etudes/BRIE/2018/630267/EPRS\\_BRI\(2018\)630267\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2018/630267/EPRS_BRI(2018)630267_EN.pdf)
- <sup>xxvii</sup> US Securities and Exchange Commission Rule 21F-17(a)
- <sup>xxviii</sup> <https://www.sec.gov/whistleblower/retaliation>
- <sup>xxix</sup> United States of America, 1984. Federal Acquisition Regulation, Sub-part 22.15
- <sup>xxx</sup> United States of America, 2015. Federal Acquisition Regulation; Ending Trafficking in Persons.
- <sup>xxxi</sup> 52.222-50(h)(3)(ii). Emphasis added.
- <sup>xxxii</sup> BSR, 2020. Human Rights and Anti-Corruption: Making the link more explicit. Written inputs to the UN Human Rights Council.
- <sup>xxxiii</sup> For example, Step 5 of the Gold Supplement of the OECD’s Guidance (p. 111) notes that companies should “Annually report or integrate into annual sustainability or corporate responsibility reports, additional information on due diligence for responsible supply chains of gold from conflict-affected and high-risk areas, with due regard taken of business confidentiality and other competitive or security concerns.” The footnote (59) to this text explains that “explains that business confidentiality and other competitive or security concerns means, without prejudice to subsequent evolving interpretation: price information; supplier identities and relationships (however the identity of the refiner and the local exporter located in red flag locations should always be disclosed except in cases of disengagement); transportation routes; and the identity of information sources and whistle-blowers located in conflict-affected and high-risk areas, where revealing the identity of such sources would threaten their safety. All information will be disclosed to any institutionalised mechanism, regional or global, once in place with the mandate to collect and process information on minerals from conflict-affected and high-risk areas.”
- <sup>xxxiv</sup> EU Human Rights Due Diligence Legislation: Monitoring, Enforcement and Access to Justice for Victims (Briefing requested by the DROI Subcommittee (June 2020), p. 7
- <sup>xxxv</sup> Ibid., p. 1.
- <sup>xxxvi</sup> EU Human Rights Due Diligence Legislation: Monitoring, Enforcement and Access to Justice for Victims (Briefing requested by the DROI Subcommittee (June 2020), p. 11.
- <sup>xxxvii</sup> EU Human Rights Due Diligence Legislation: Monitoring, Enforcement and Access to Justice for Victims (Briefing requested by the DROI Subcommittee (June 2020), p. 12.
- <sup>xxxviii</sup> Article 7 article (Protection of employees’ representatives) requires Member States to ensure that employees’ representatives, when carrying out their functions, enjoy adequate protection and guarantees to enable them to perform properly the duties which have been assigned to them.
- <sup>xxxix</sup> Article 23 notes that “The definition of ‘consultation’ needs to take account of the goal of allowing for the expression of an opinion which will be useful to the decision-making process, which implies that the consultation must take place at such time, in such fashion and with such content as are appropriate.” Article 34 highlight that provisions should be made for the employees’ representatives acting within the framework of this Directive to enjoy, when exercising their functions, the same protection and guarantees as those provided to employees’ representatives by the legislation and/or practice of the country of employment. They must not be subject to any discrimination as a result of the lawful exercise of their activities and must enjoy adequate protection as regards dismissal and other sanctions. Article 36 suggests that in accordance with the general principles of Community law, administrative or judicial procedures, as well as sanctions that are effective, dissuasive and proportionate in relation to the seriousness of the offence, should be applicable in cases of infringement of the obligations arising from this Directive.
- <sup>xl</sup> Article 10 establishes that members of the special negotiating body, the members of the representative body, any employees’ representatives exercising functions under the information and consultation procedure and any employees’ representatives in the supervisory or administrative organ of an SE who are employees of the SE, its subsidiaries or establishments or of a participating company shall, in the exercise of their functions, enjoy the same protection and guarantees provided for employees’ representatives by the national legislation and/or practice in force in their country of employment. This shall apply in particular to attendance at meetings



of the special negotiating body or representative body, any other meeting under the agreement referred to in Article 4(2)(f) or any meeting of the administrative or supervisory organ, and to the payment of wages for members employed by a participating company or the SE or its subsidiaries or establishments during a period of absence necessary for the performance of their duties.

<sup>xli</sup> Section 7 of the UK Anti-Bribery Act (2010) took a new approach to corporate criminal liability by making companies criminally liable for failing to prevent bribery by associated persons (subject to a compliance defense of having 'adequate' anti-bribery procedures in place).

<sup>xlii</sup> Remaining anonymous is one potential strategy to address risks of retaliation, and often the default option to protect individuals and organisations from being exposed to harm. Nevertheless, depending on the context and the preferences of those at risk, other strategies may be a better option to prevent or mitigate risks, including, for example issuing public statements recognizing their right to express freely their opinion or communicating clearly to the companies concerned, at the outset of a complaints handling process, investigation or other procedure that retaliation will not be tolerated.

<sup>xliii</sup> Section 7 of the UK Anti-Bribery Act (2010) took a new approach to corporate criminal liability by making companies criminally liable for failing to prevent bribery by associated persons (subject to a compliance defense of having 'adequate' anti-bribery procedures in place).