THE BUSINESS'S COMMERCIAL SUCCESS SUBSTANTIALLY DEPENDS UPON:

RED FLAG NO. 9

WITH AI & DATA LENS

RED FLAGS IN THE VALUE PROPOSITION

Offering **products or services with the potential for harmful forms of use**, especially by end-users that are inclined to pursue those uses.

**Such as:**

- **Selling "dual use" products, services or technology (such as those normally used for civilian purposes, but which may also have military applications)**
- **Providing tracking or facial recognition technologies that may be misused to profile, intimidate or arbitrarily imprison human rights defenders or activists**
- **Providing pharmaceuticals that may be misused for the death penalty**
- **Providing heavy machinery or equipment to governments for use in locations recognized under international law as occupied territories**
- **Selling ultrasound technology to health facilities that may misuse it for sex selective abortions**
- **Providing social media platforms, that may be misused for harassment or to incite hatred (see also red flag 6)**

## HIGHER-RISK SECTORS:

- ICT, in particular, surveillance technologies, social media and telecommunications
- Pharmaceuticals
- Heavy Machinery
- Chemical
- Medical technology
- Geographies with a record of abuses of a type relevant to the company's product or service

## KEY QUESTIONS FOR LEADERS TO ASK OR BE ASKED:

- How does the company find out about, and keep up to date on, the risk of its products being used in ways that impact human rights?
- What safeguards and procedures are in place to prevent and mitigate situations of harmful use of products?
- How does the company assess whether intermediaries or agents are likely to facilitate harmful product/service misuse by end users?
- How does the company ensure that incentives to maximize sales and other business opportunities do not reduce the chances of identifying and preventing harmful use of products or services?

THE BUSINESS'S COMMERCIAL SUCCESS SUBSTANTIALLY DEPENDS UPON:

RED FLAG NO. 9

WITH AI & DATA LENS

RED FLAGS IN THE VALUE PROPOSITION

Offering **products or services with the potential for harmful forms of use**, especially by end-users that are inclined to pursue those uses.

HIGH-LEVEL DECISION-MAKING

RISK TO PEOPLE

RISK TO THE BUSINESS

UNGPs & SGDs ANALYSIS

TAKING ACTION

## RISKS TO PEOPLE

- Risks to people are heightened by the nexus between products that are vulnerable to harmful use and sales to entities likely to use them in rights impacting ways. Where patterns of misuse are well understood, treating them as externalities risks overlooking how business decisions may **enable or profit from those outcomes.**
- Interviews with business and civil society representatives conducted by the UN Global Compact "underscored that one of the biggest challenges in conceptualizing product misuse as a human rights issue is the vast array of ways, including non-obvious ways, a product or service can be misused and inflict human rights harm."
- Several examples are listed above and include severe impacts, such as sale of pharmaceuticals misused for the administration of the death penalty (*right to life; right to freedom from torture, cruel, inhuman or degrading treatment*).
- An area of particular challenge in the space of harmful product use is dual-use technology, and in particular emerging defense technologies. **Dual use technology** can be used, for example, in weapons – including autonomous weapons - and surveillance technology. Dual-use technologies have the potential to cause some of the most severe human rights violations, in particular, in the context of repressive state action or conflict.
  - **Autonomous weapon systems** are "designed to select and engage one or more targets without the need for human intervention after activation". Weapons that are by nature incapable of being used in compliance with the international humanitarian law (IHL) principles[1] of 'distinction', 'proportionality' and 'precaution' in the context of a military attack are understood to raise acute legal and human rights concerns. Where technologies can be adapted or incorporated into these systems, they become connected to an increased risk of civilian harm and weaken the safeguards intended to protect people in armed conflict. Products described broadly as providing "situational awareness," "object recognition," or "decision support" in military contexts may ultimately support targeting operations: AI-enabled decision-support systems can accelerate targeting processes beyond meaningful human control, compressing human judgment and potentially increasing both the scale and speed of operations in ways that heighten risks to civilians.
  - **Surveillance technologies** can also give rise to severe harms to people when used by repressive states, including for arbitrary detention, torture, enforced disappearances and the suppression of fundamental freedoms such as expression, association and privacy. The aggregation and analysis of personal data can enable the identification, tracking and targeting of individuals or groups at scale, increasing risks of discrimination, persecution and abuse *(freedom from arbitrary arrest, detention or exile and/or freedom from torture and inhuman or degrading treatment).*

[1] IHL comprises the body of international law that regulates the conduct of parties in an armed conflict and is reflected most prominently in the four Geneva Conventions and their Additional Protocols and so-called 'customary IHL'. These laws include rules on the protection of civilians and restrictions on the means and methods of warfare, and apply to aggressors as well as those engaged in legitimate self-defense.

## THE BUSINESS'S COMMERCIAL SUCCESS SUBSTANTIALLY DEPENDS UPON:

Offering **products or services with the potential for harmful forms of use**, especially by end-users that are inclined to pursue those uses.

RED FLAG NO. 9

WITH AI & DATA LENS

RED FLAGS IN THE VALUE PROPOSITION

HIGH-LEVEL DECISION-MAKING

RISK TO PEOPLE

RISK TO THE BUSINESS

UNGPs & SGDs ANALYSIS

TAKING ACTION

### RISKS TO THE BUSINESS

- **Reputational and Legal Risks:** Links between well-known companies and the impacts of harmful product use are more easily spread through the 24/7 news cycle and the sharing of incidents and photographs facilitated by mainstream and social media. During the Arab Spring, the role of Western Technology firms in "helping Arab dictators" was highlighted in US media. Popular opinion increasingly places some degree of responsibility on the companies concerned, and not just on those using the product or service, or on regulators.
  - The use of AI-supported weapons and dual-use technology is attracting increasing scrutiny and creating heightened reputational exposure for companies linked to conflict-affected contexts. A June 2025 report by UN Special Rapporteur Francesca Albanese, titled "From economy of occupation to economy of genocide", examines the role of corporate actors in relation to Israel's occupation of Palestinian Territories and military operations in Gaza. The report alleges that certain corporate activities and transfers of weapons, surveillance capabilities and "dual-use" technologies may be connected to alleged violations of international law, including concerns relating both to the conduct of hostilities in Gaza and to the expansion of settlements in the occupied West Bank. The report was based on over 200 submissions, creating a database of roughly 1,000 corporate entities. It emphasized that products and services not formally classified as weapons, but capable of serving military, surveillance or security purposes, can nonetheless play a significant role in sustaining military operations and occupation-related infrastructure. The report named companies providing products and services such as technology and surveillance, spyware, transport and infrastructure, tourism and energy supply. It was reported that more than 45 entities were informed of the allegations and invited to respond, of which 15 replied.

- **Operational and reputational risks:** Amazon's Ring provides a recent illustration of how business partnerships can rapidly convert product features into privacy risks with significant reputational and operational consequences. A Super Bowl ad promoting Ring's AI-powered "Search Party" feature — designed to locate lost dogs by scanning a network of neighborhood cameras — triggered immediate public backlash when viewers recognized that the same technology, combined with Ring's existing facial recognition capability and a planned integration with police surveillance company Flock Safety, could readily be repurposed to track people. Within days, Amazon terminated the Flock partnership and faced a Congressional letter raising concerns about Ring's surveillance capabilities and invasive image recognition algorithms.

- **Operational and regulatory risks:** Developers of AI image generation tools have faced regulatory scrutiny and platform restrictions following misuse of their technologies to create non-consensual or harmful synthetic content, including deepfake images. In response, companies have been required to introduce safeguards, while facing operational constraints and reputational pressure.

THE BUSINESS'S COMMERCIAL SUCCESS SUBSTANTIALLY DEPENDS UPON:

Offering **products or services with the potential for harmful forms of use**, especially by end-users that are inclined to pursue those uses.

RED FLAG NO. 9

WITH AI & DATA LENS

RED FLAGS IN THE VALUE PROPOSITION

## RISKS TO THE BUSINESS

- **Financial Risks:** May include investor divestment or customer boycotts where companies are seen to be failing to address product misuse.
  - For example, Norwegian pension fund KLP has divested from companies including Caterpillar, citing concerns about the use of their products in contexts associated with human rights harms, including in the occupied Palestinian territories. In 2012, MSCI removed Caterpillar from several ESG indexes following an ESG rating downgrade. According to MSCI, one of the "key factors" was "an on-going controversy associated with use of the company's equipment in the occupied Palestinian territories."
  - In March 2026 Canadian shareholder association SHARE, together with Parnassus Investments and Denmark's PFA Pension, filed a proposal at Alphabet calling on the company to update the charter of its board's audit committee to provide format oversight on AI-related risks and the responsible development and deployment of AI, which may impact the human rights of users and other stakeholders.
  - Analysis published by Business and Human Rights Centre (BHRC), in partnership with Open MIC and others highlights growing investor concern about exposure to high-risk AI systems linked to defense and conflict settings. The research found that at least 182 public and private pension funds are invested in companies developing high-risk AI systems with military applications. The authors warn that existing ESG screens and due diligence approaches are often insufficient to identify and address risks arising from the foreseeable harmful use of defense and dual-use products. They group calls for strengthened due diligence, disclosure, and clear red lines around unacceptable uses.
  - Investors and market participants working on a set of Principles for Responsible Defence Investment – rebranded in early 2026 as Guidance for Responsible Investment in Defence-related Companies (GRID) – in order to focus on **investor due diligence on downstream product use.**

- **Legal, Financial and Operational Risks:** For example, where end users include repressive regimes.
  - Blacklisting of Chinese technology companies by the US Government on the grounds of rights violations against Muslim minority groups in Xinjiang, China, disallows US companies from selling technology to these companies without a US government license. In 2019, Sony and Sharp faced scrutiny for the alleged supply of parts to a Chinese video surveillance company blacklisted by the United States over human rights violations of ethnic Uyghur people in the Xinjiang Autonomous Region of China. The blacklisted company had "previously stated on its website that it could identify members of the Uighur ethnic minority group." In 2023, the US Government expanded its export controls to restrict the sale of advanced semiconductors and chipmaking equipment to China, citing risks of military and surveillance end-use, including use in repression.





Shift

THE BUSINESS'S COMMERCIAL SUCCESS SUBSTANTIALLY DEPENDS UPON:

Offering **products or services with the potential for harmful forms of use**, especially by end-users that are inclined to pursue those uses.

RED FLAG NO. 9

WITH AI & DATA LENS

RED FLAGS IN THE VALUE PROPOSITION



## RISKS TO THE BUSINESS

- **In the specific context of defense and conflict**, it is important to note that **legal risks** arise pursuant to potential violations of international humanitarian law (see footnote 1). Concrete legal risks arise for businesses and individual corporate actors, including directors, executives and other decision-makers, in circumstances where their activities are 'closely linked' to an armed conflict.
    - Companies have faced direct legal exposure for alleged involvement in international crimes, including war crimes. Swedish prosecutors have charged executives of Lundin Energy with complicity in war crimes linked to operations in Sudan. Chiquita Brands International pleaded guilty in the United States to financing a paramilitary group responsible for widespread violence against civilians in Colombia. Even where cases are not framed as war crimes, companies face exposure linked to harms governed by international humanitarian law. Lafarge pleaded guilty in the United States to providing material support to armed groups in Syria. Meta has faced litigation brought by Rohingya plaintiffs over alleged incitement to violence in Myanmar.
    - **Financial institutions** have also faced judicial and quasi-judicial scrutiny for alleged links to serious conflict-related harms. BNP Paribas has been subject to ongoing U.S. litigation concerning its provision of financial services to the Sudanese government during the Darfur conflict, while cases such as Jesner v. Arab Bank and civil society analyses of banking activity in Israeli settlements illustrate the growing willingness of courts and stakeholders to test financial institutions' potential exposure to international humanitarian law-related risks. Norges Bank Investment Management has faced sustained scrutiny in Norway, including a 2026 criminal complaint alleging that the oil fund's investments in certain companies may contribute to IHL crimes in Gaza, underscoring the increased public scrutiny of investor responsibilities in conflict-affected contexts.

**THE BUSINESS'S COMMERCIAL SUCCESS SUBSTANTIALLY DEPENDS UPON:**

Offering **products or services with the potential for harmful forms of use**, especially by end-users that are inclined to pursue those uses.

RED FLAG NO. 9

WITH AI & DATA LENS

RED FLAGS IN THE VALUE PROPOSITION

HIGH-LEVEL DECISION-MAKING

RISK TO PEOPLE

RISK TO THE BUSINESS

UNGPs & SGDs ANALYSIS

TAKING ACTION

## WHAT THE UN GUIDING PRINCIPLES SAY:

This red flag arises in two distinct situations, namely where the business relies on:

a) sales to a known commercial customer where there is a likelihood it will use or misuse the product in ways that have human rights impacts, or sell it onwards to an end-user who misuses the product; and

b) sale of a product or service to the general public, where there is foreseeable misuse by a minority.

With regards to scenario a), Guiding Principle 13(b) states that businesses should "seek to prevent or mitigate adverse human rights impacts that are **directly linked** to their operations, **products or services** by their business relationships, even if they have not contributed to those impacts." Business relationships include relationships with commercial *customers*, and as such, a company may be **directly linked** to an impact caused by commercial customers in the course of using the product or service.

In certain circumstances, harmful use by a commercial customer may involve a situation of **contributing** to harm where a company knows of the risk or fact of its products being used in this way, and does nothing to address the situation. The UN Global Compact describes a scenario in which a company sets up a shell company in order to hide the fact that it is selling surveillance technology to repressive governments. If the company knew or should have known that the governments concerned were likely to use the product to impact human rights, yet proceeded with a sale that enables this, it may be considered to **contribute** to any harm suffered.

In scenario b), the scope of the company's human rights responsibility includes the safety of people using its products, even if they are not the intended user. As such, if the company is – or should be – aware of a potential negative impact associated with its products, a failure to adapt the product or otherwise seek to minimize the risk of the impacts occurring (e.g. through terms and conditions of use, warnings on packaging or instructions etc.) could place the company in a situation of **causing** an impact, or, where the impact on a third party is caused by a consumer misusing its products, **contributing to the impact**.







Shift

## THE BUSINESS'S COMMERCIAL SUCCESS SUBSTANTIALLY DEPENDS UPON:

Offering **products or services with the potential for harmful forms of use**, especially by end-users that are inclined to pursue those uses.



## POSSIBLE CONTRIBUTIONS TO THE SDGS:

Addressing impacts to people associated with this red flag indicator can contribute to a range of SDGs depending on the industry and impact concerned, for example:

**SDG 3: Good Health and Well-Being**

**SDG 9: Industry, innovation and infrastructure,** in particular

- **Target 9.1:** Develop quality, reliable, sustainable and resilient infrastructure, including regional and transborder infrastructure, to support economic development and human well-being, with a focus on affordable and equitable access for all.

**SDG 10: Reduced Inequalities,** in particular

- **Target 10.2:** By 2030, empower and promote the social, economic and political inclusion of all, irrespective of age, sex, disability, race, ethnicity, origin, religion or economic or other status.

**SDG 11: Sustainable Cities and Communities,** in particular

- **Target 11.3:** By 2030, enhance inclusive and sustainable urbanization and capacity for participatory, integrated and sustainable human settlement planning and management in all countries.

**SDG 12: Responsible Consumption and Production**

**SDG 16: Peace, Justice and Strong Institutions,** in particular

- **Target 16.1:** Significantly reduce all forms of violence and related death rates everywhere.
- **Target 16.6:** Develop effective, accountable and transparent institutions at all levels.
- **Target 16.7:** Ensure responsive, inclusive, participatory and representative decision-making at all levels.

HIGH-LEVEL DECISION-MAKING

RISK TO PEOPLE

RISK TO THE BUSINESS

UNGPs & SGDs ANALYSIS

TAKING ACTION

## THE BUSINESS'S COMMERCIAL SUCCESS SUBSTANTIALLY DEPENDS UPON:

Offering **products or services with the potential for harmful forms of use**, especially by end-users that are inclined to pursue those uses.

RED FLAG NO. 9

AI WITH AI & DATA LENS

RED FLAGS IN THE VALUE PROPOSITION

## DUE DILIGENCE LINES OF INQUIRY:

**Risk identification & Governance**

- How do we assess the potential risk of harmful use of our products? How do we understand and address the ways in which "specific variables in design, components or materials used, and markets and customers targeted" may lead to harmful use resulting in human rights impacts?
- How do we ensure that we understand our **indirect exposure to harmful use**, including through minority stakes, intermediaries or complex ownership structures?
- How do we assess **foreseeable use in conflict-affected or high-risk contexts?**
- **[On AI]** How do we address risks arising from **limited transparency in AI systems**, including "black box" models whose internal decision-making processes may obscure harmful uses or impacts?
- What internal processes exist to **escalate concerns about harmful use**, and who is accountable for decisions to continue, restrict or exit business relationships with high-risk customers or end-users?

**Customers and End Use**

- How do we know which of our end users/customers are high risk from the perspective of harmful use? How do we stay abreast of developments that affect the level of risk? What systems do we have in place to identify and address such risks, prior to sale?
- Do we build safeguards against product misuse/harmful use into our agreements with business customers, end-users and intermediaries involved in the sale of our products/services? Under what conditions would we **restrict, suspend or terminate** relationships based on evidence or risk of harmful use?
- What contractual mechanisms do we have to **monitor downstream use in practice**, particularly where products are deployed in conflict-affected or high-risk environments?
- How do we increase **traceability and auditability** of how our products or systems are used once deployed?

**Leverage/Policy Engagement**

- Has the company considered how it might work with others – regulators, industry peers, customers, civil society organizations etc. – to seek ways to **minimize the potential harmful use** of its products?
- Do we engage publicly or collaboratively to **shape market norms** around responsible use of high-risk or dual-use technologies?

THE BUSINESS'S COMMERCIAL SUCCESS SUBSTANTIALLY DEPENDS UPON:

Offering **products or services with the potential for harmful forms of use**, especially by end-users that are inclined to pursue those uses.

RED FLAG NO. 9

WITH AI & DATA LENS

RED FLAGS IN THE VALUE PROPOSITION

HIGH-LEVEL DECISION-MAKING | RISK TO PEOPLE | RISK TO THE BUSINESS | UNGPs & SGDs ANALYSIS | TAKING ACTION

## DUE DILIGENCE LINES OF INQUIRY:

**Transparency**

- How do we track and report internally or externally on our efforts to ensure responsible use of our products and/or services?

**Spotlight on defense**

- How do we identify and address **dual-use characteristics** of our products and services, including where civilian applications may be repurposed for military, intelligence or security uses?
- Is our due diligence informed by an understanding of the lifecycle of the relevant weapons systems, including considering impacts associated with:
  - Known or likely end-users;
  - Research and development (including battle testing);
  - The responsible design and deployment of dual-use products; and
  - Risks of diversion of weapons (the risk that weapons are transferred, captured, stolen, or otherwise end up in the hands of unintended or unauthorized users), whether within or beyond a given conflict?
- What visibility do we have over how our products are **marketed or positioned to defense, national security or intelligence clients**, whether directly or through partners?
- Do we include reference to the need for use that respects international humanitarian law into our contracts and policies? What accountability is there for implementation of such clauses?

Do we allocate **sufficient internal resources** or readily available external expertise to remain abreast of developments on dual use technology that are relevant to our involvement with impacts on people?

**Spotlight on pension funds and AI systems:**

A report containing analysis conducted by Empower in partnership with the BHRC, Open MIC and Heartland Initiative, provides the following key recommendations for pension fund managers undertaking due diligence on their connection to "high-risk AI systems".

- "Tie capital commitments to data governance safeguards that force the decoupling of civilian and military data
- Require human rights and humanitarian law risk disclosure from general partners (GP) and big tech companies
- Embed human rights due diligence into GP contracts and processes
- Draw red lines, abstain from high-risk AI investments, and ensure that GPs are actively mitigating risks to civilians in their investment decisions
- Engage publicly and collaboratively to reshape market norms around responsible AI toward deescalation and a 'do no harm' approach".

## THE BUSINESS'S COMMERCIAL SUCCESS SUBSTANTIALLY DEPENDS UPON:

Offering **products or services with the potential for harmful forms of use**, especially by end-users that are inclined to pursue those uses.

RED FLAG NO. 9

WITH AI & DATA LENS

RED FLAGS IN THE VALUE PROPOSITION

### MITIGATION EXAMPLES:

* Mitigation examples are current or historical examples for reference, but do not offer insight into their relative maturity or effectiveness.

Where the red flag relates to **sales to a known commercial or government customer where there is a likelihood they will use the product/services in ways that have human rights impacts**, mitigation has involved

- attempting to influence or constrain their use of the product;
- limiting sales to that customer; and/or
- hiring technical experts to understand and mitigate foreseeable risks relating to misuse.

These examples illustrate that mitigation often involves trade-offs, particularly where misuse is commercially valuable or aligned with powerful customer interests.

- **Misuse of technology to target weapons autonomously and conduct surveillance:** The US Pentagon's dispute with Anthropic stems from the AI startup's refusal to remove safeguards that would prevent its technology from being used to target weapons autonomously and conduct surveillance in the United States. This issue highlights that national security priorities do not automatically resolve responsible-use questions, and even where governments invoke security imperatives, companies can resist proposals that would weaken safeguards on the development of powerful technologies. Anthropic's refusal resulted in the loss of a major government contract and subsequent legal dispute. At the same time, the company experienced a surge in user adoption and revenue and more than 875 employees across Google and OpenAI signed an open letter backing Anthropic's stance.
- As a further example of mitigation in this area, it has been reported that **AI firms are seeking technical experts to manage the potential for harm related to misuse:** Anthropic has been looking to hire a chemical weapons and high-yield explosives expert to try to prevent "catastrophic misuse" of its software, and ChatGPT advertised for a researcher in biological and chemical risks.
- In 2025, media investigations alleged that Microsoft's Azure cloud infrastructure was being used by Israel's military intelligence unit, Unit 8200, to store and process large volumes of intercepted Palestinian communications. Microsoft stated that it had not been aware of this use, launched an external review, and assessed the allegations against its terms of service, including its prohibition on using Microsoft technology for mass surveillance of civilians. Following the review, Microsoft concluded that aspects of the use violated its terms and disabled specific cloud and AI services used by the unit. Microsoft subsequently announced changes to strengthen oversight of high-risk government and national security customers, including enhanced due diligence, monitoring and governance processes.

## THE BUSINESS'S COMMERCIAL SUCCESS SUBSTANTIALLY DEPENDS UPON:

Offering **products or services with the potential for harmful forms of use**, especially by end-users that are inclined to pursue those uses.

RED FLAG NO. 9

WITH AI & DATA LENS

RED FLAGS IN THE VALUE PROPOSITION

### MITIGATION EXAMPLES:

* Mitigation examples are current or historical examples for reference, but do not offer insight into their relative maturity or effectiveness.

- **Misuse of facial recognition technology:** Major cloud providers including Microsoft, Amazon and Google have at various points imposed restrictions on the use of facial recognition technologies by law enforcement or government actors, including moratoria, contractual limitations and requirements for human rights review. These measures were introduced in response to concerns about discriminatory impacts and misuse in surveillance contexts, demonstrating efforts to constrain foreseeable harmful uses by state customers.

- **Use of financing for rights-impacting activities:** Investors, lenders, insurers and providers of export credit also look to restrict the use of their financial products and services in ways that can impact rights. A number of financial institutions explicitly reference the need for clients in the defense sector to respect international humanitarian law or closely related legal standards. For example, La Banque Postale, ABN AMRO and BNP Paribas in Europe, as well as DBS in Asia, reference IHL or "humanitarian principles" rooted in IHL, humanitarian disarmament treaties (such as those prohibiting cluster munitions and anti-personnel mines), or related international conventions, when setting financing criteria and due diligence expectations.
  - The Collective Impact Coalition for Ethical Artificial Intelligence (AI CIC), brings together investors, civil society organizations (CSOs), and other stakeholders to press companies for stronger policies, governance structures, and disclosures that can shed light on their commitments and operationalization of responsible AI.

- **Misuse of Pharmaceutical Drugs for the Death Penalty:** Drug companies have adopted controls on the distribution of their products to ensure that none are used in lethal injections. In 2016 Pfizer announced that it will restrict the sale of relevant drugs to selected wholesalers who must certify that they will not resell the drugs to corrections departments in the United States. Following Pfizer's announcement it was reported that all Food and Drug Administration-approved manufacturers of any potential execution drugs have blocked their sale for the purpose of lethal injection.

- **Misuse of Ultrasound Technology in Sex-selective Abortions:** GE discovered that its portable ultrasound machines, which enable access to life-saving medical treatment in remote regions, were being used by some facilities in India, in contravention of local law, to determine the sex of fetuses to enable early abortion of those that are female. This reflected strong social preferences for male children in India. In response, the company strengthened training to sales agents, added an explicit warning about national legal requirements in all sales contracts and on the machines themselves, engaged with NGOs and other local stakeholders, pushed for industry-wide collaboration and collaborated in a public education campaign on women and girls' rights.

THE BUSINESS'S COMMERCIAL SUCCESS SUBSTANTIALLY DEPENDS UPON:

Offering **products or services with the potential for harmful forms of use**, especially by end-users that are inclined to pursue those uses.

RED FLAG NO. 9

WITH AI & DATA LENS

RED FLAGS IN THE VALUE PROPOSITION

HIGH-LEVEL DECISION-MAKING

RISK TO PEOPLE

RISK TO THE BUSINESS

UNGPs & SGDs ANALYSIS

TAKING ACTION

## MITIGATION EXAMPLES:

* Mitigation examples are current or historical examples for reference, but do not offer insight into their relative maturity or effectiveness.

- Industrial manufacturer Honeywell International found a way to make a safer alternative to ammonium nitrate that was designed to be hard to ignite, after the fertilizer was used in a bomb that killed 168 people in Oklahoma.
- WhatsApp introduced limits on message forwarding and labels for forwarded messages in response to misuse of the platform to spread misinformation and incite violence, particularly in contexts such as India and Brazil.
- Platforms such as YouTube and TikTok have adjusted recommendation algorithms and introduced friction (e.g. content warnings, removal, demonetization) to reduce the spread of harmful or misleading content, including through labelling, removal of content and limiting distribution in response to concerns about misinformation and harmful influence.
- Drone manufacturer DJI has implemented geofencing and other technical controls to restrict the use of its drones in sensitive locations (such as airports, government sites etc), and has taken additional steps such as suspending operations in conflict-affected areas, in response to concerns about misuse for military or harmful purposes.

THE BUSINESS'S COMMERCIAL SUCCESS SUBSTANTIALLY DEPENDS UPON:

Offering **products or services with the potential for harmful forms of use**, especially by end-users that are inclined to pursue those uses.

RED FLAG NO. 9

WITH AI & DATA LENS

RED FLAGS IN THE VALUE PROPOSITION



## OTHER TOOLS AND RESOURCES:

- UN Global Compact Good Practice Note, prepared by Meaghan Malloy (2017) *Addressing Adverse Human Rights Impacts Connected to Product Misuse*. [1]
- Human Rights and Business Dilemmas Forum, *Product Misuse dilemma* sets out common product misuse scenarios, case examples, risks to business and suggestions for responsible business.
- Bureau of Democracy, Human Rights, and Labor, U.S. Department of State Guidance on Implementing the "UN Guiding Principles" for Transactions Linked to Foreign Government End-Users for Products or Services with Surveillance Capabilities.
- The IEEE SA Industry Connections Research Group on Issues of Autonomy and AI in Defense Systems has created a Framework For Human Decision-Making Through the Lifecycle of Autonomous and Intelligent Systems in Defense Applications(2024). The framework provides "a granular means for identifying the technical considerations that are necessary to meet legal requirements, to inform and guide ethical discussions, and to determine human responsibility and accountability across the entire lifecycle of autonomous and intelligent systems".
- In May 2023, the Responsible Investment Association Australasia (RIAA) released its Investor Toolkit on Human Rights and Armed Conflict – one of the first guides written by investors for investors on the topic.
- Saving for the future or threatening the future: are pensioners funding the militarisation of AI? (Business & Human Rights Resource Centre, with Open MIC, Heartland Initiative and Empower) – Examines investor exposure to companies developing AI systems for military and intelligence use, highlighting gaps in due diligence and calling for stronger safeguards around dual-use risks.

This resource is part of Shift's collection of Business Model Red Flags, developed as part of the Valuing Respect Project and generously funded by Ministry of Foreign Affairs Finland, the Norwegian Ministry of Foreign Affairs, and Norges Bank Investment Management. The resource was updated during 2025-26 with generous funding from Generation Foundation. Learn more at: shiftproject.org/valuing-respect

[1] Several examples in this red flag are drawn from this UN Global Compact Good Practice Note