

To: Spanish Presidency of the Council of the European Union; Ms. Lara Wolters, Rapporteur for the European Parliament; Mr. Didier Reynders, Commissioner for Justice

December 2023

Honourable decision-makers,

As the Trilogue negotiations on the Corporate Sustainability Due Diligence Directive (CSDDD) reach concluding stages, the Business & Human Rights Resource Centre repeats its call for **the CSDDD to cover the full value chain, including downstream, so technology companies can be effectively held accountable for human rights and environmental abuses.**

In alignment with the international [UN](#) and [OECD](#) standards, companies have a responsibility to conduct human rights due diligence (HRDD) across their entire value chains. **This is especially crucial for due diligence in the technology sector, where many of the most [severe human rights risks](#) are present in the downstream value chain. [Many technology companies](#) and [investors](#) already recognise this, but companies still [do not have enough of an incentive](#) to act on the voluntary standards to which they have agreed. The EU needs to level the playing field and require that companies mitigate risks to our economies, human rights, and democracies.**

To be most effective, the CSDDD should require that companies carry out risk-based HRDD regarding the downstream impacts of their technology products and services, including impacts resulting from their design, development, marketing, sale, deployment, use, maintenance and disposal by themselves or others. **We have followed with concern the attempts to narrow the CSDDD's downstream value chain concept, especially by the Council, and urge you to conclude provisions that cover technology impacts downstream comprehensively.** This includes cases where products are already subject to export control rules, as these are all too often evaded in practice, e.g. by downstream business partners. **A directive that does not require companies whose most salient human rights and environmental impacts are downstream to address these, will fail to establish a full risk-based approach and a level playing field between all types of companies.**

While we understand that there are other pieces of legislation that will impact the technology sector, such as the [EU AI Act](#), **these pieces of legislation complement each other; they are not repetitive, nor should they be treated as a replacement for the other.** As the CSDDD is not specific to any kind of technology, it is best placed to address the future evolution of this high-impact sector. There is misleading information circulating that legislations are overlapping, and we are concerned that misinterpretation may lead to dangerous carve-outs across all files, ultimately resulting in protection gaps. It is an entirely proportionate and necessary ask that technology companies carry out HRDD and disclose information in a way that complies with complementary legislation; for example, by consolidating all HRDD information about ongoing work concerning data privacy impact assessments to comply with the General Data Protection Regulation (GDPR). It is easier to creatively develop new means of effective and meaningful due diligence reporting, and most importantly action, than it is to reconcile irremediable harms.

1) Full downstream HRDD is necessary to fill the gaps in existing and pending EU regulations that address the negative impacts of technology.

The EU's recent agreement on the [Artificial Intelligence Act \(AIA\)](#) has requirements that [leave gaps](#) concerning accountability and remediation for abuses experienced by rights-holders. This is [especially true](#) for rights-holders outside of the EU. Just as the GDPR is an [essential complement](#) to the AIA for

mitigating abuses of the right to privacy, downstream due diligence mandated by the CSDDD is an essential complement for mitigating technology sector abuses of other human rights, including the right to health, freedom of expression, the right to a fair trial, freedom of movement (particularly for [refugees and asylum seekers](#)) and the right to life.

2) To prevent abuse, technology companies must consider the potentially nefarious end-uses of their products and services before engaging with high-risk clients or in high-risk contexts.

Mandatory downstream HRDD is an opportunity for European governments to address technologies that [pose a global threat to human rights and democracy](#). Surveillance technologies, like spyware, have grave and [sometimes irreparable impacts](#) on the end-user. Of the [cases that have come to light](#), at least [14 world leaders](#), numerous [government officials](#) and [allies](#) have been identified as potential spyware targets, putting their security and rights at risk. Spyware is too high-risk a technology for private sector actors to be left to self-govern what is considered to be an acceptable use.

At present, spyware providers have little obligation to scrutinise repeat customers to determine whether their use of the technology is legitimate or illegitimate. Downstream HRDD in the CSDDD provides a necessary and material disincentive for turning a blind eye to the illegal or harmful use of powerful technologies further down the distribution chain.

Spyware is not the only extreme example. The same can be said for [network providers](#), social media platforms, generative AI tools, [data centres or software providers](#) and others who [do not](#) conduct human rights-centric know-your-customer due diligence.

3) The CSDDD has to complement existing [consumer protection standards](#) to ensure protection from human rights abuses after the point of sale.

Technology companies continue to engage with customers and users after the point of sale to ensure products continue to be safe and usable. This is done through the issuance of patches – software updates that are likely to include performance improvements, bug fixes, and security fixes – long beyond initial purchase. Companies invest in continual servicing ([sometimes for years until after the point of sale](#)) to protect the consumer from unwarranted intrusion into their devices and to protect their reputations from being tarnished.

This relationship of continual amenability is one of the many bases on which corporate responsibility for downstream HRDD should stand. Effectively preventing and addressing human rights abuses with effective HRDD should complement the realisation of existing [consumer protection standards](#). Requiring HRDD will ensure that companies meet evolving consumer demands for socially responsible and accountable digital technologies, and European companies have a competitive edge in the next-generation marketplace.

4) Technology companies need to conduct full downstream HRDD to build evidence for ending rights-abusing business relationships, especially during conflict.

As actual and evolving risks and human rights harms are identified and mitigation attempts are made, systematic downstream due diligence is needed to track and stop the perpetuation of harms and break cycles of corporate impunity. Companies should be required to collect evidence of nefarious end-use of their technologies to end problematic business relationships in a timely manner, consistent with the principle of responsible disengagement.

Conducting [downstream due diligence assessments](#) will better ensure that companies undergo processes of [responsible exit](#) or have strong justification for responsibly staying in challenging markets. This is

increasingly critical for technology companies' impact on human rights in [conflict settings](#), as exemplified by the [war in Ukraine](#). Technology companies play a pivotal role in times of conflict, particularly concerning connectivity to [receive information](#), the spread of [misinformation](#), and accessibility of critical [government services](#) and personal identification documents. As explained by the [OECD](#), downstream HRDD can help “improv[e] visibility over complex business relationships that heighten the risk of sanctions evasion – including in the context of export restrictions on certain dual use technologies to Russia.”

5) Full downstream HRDD is necessary to ensure that the strength of CSDDD protections remains relevant for the technology sector.

Technology is evolving quickly and so are the ways of using it. Requiring downstream due diligence for technology companies in the CSDDD will help prevent harmful situations that we have yet to hypothesise or fully understand. Prior to the invention of 3D printing, legislators were unconcerned about whether people would be [printing unregistered weapons](#) within their own homes. It is now [impossible to ignore](#) the potential impacts [generative artificial intelligence](#) will have on [democratic processes](#), the [targeting of politicians](#) and [freedom of speech](#).

The impacts on the end-user for biometric surveillance technologies (including so-called [emotional intelligence](#) or [brain-computer interface](#) technologies) are yet to be fully understood. Last year, France's data protection authority warned [against the use of digital technologies for employee monitoring](#), arguing that it could lead to the permanent worker surveillance and a form of psychological harassment. Scholars continue to [argue against](#) the use of biased and pseudoscientific emotional intelligence facial recognition technologies for the purpose of [criminology and policing](#). Now, we are faced with the yet-to-be-imagined applications of generative artificial intelligence, and some companies are already [applying it to autonomous weapons systems](#).

The injustices that [minorities are experiencing](#) are being amplified in new ways as a result of under-regulated technology, including by [mis-assigning gender identities](#) and further disposing LGBTQ+ persons to risk. For the CSDDD's potency to last beyond current and future [technological arms races](#), it must consider the impacts on the most at-risk and vulnerable end-users that are often forgotten by technology companies in the design, development, sale, deployment and product maintenance stages.

As we continue to learn about the new and compounding risks associated with advanced technologies, the CSDDD must include an approach to HRDD that [includes the entire value chain](#), adopting a risk-based, human-centric approach to ensure that the legislation continues to be fit for purpose. Narrowing downstream due diligence within the CSDDD could prevent this ground-breaking legislation from realising its full potential as a true model for the rest of the world, as other jurisdictions begin drafting corporate accountability legislation.

We remain available for further dialogue and assistance.

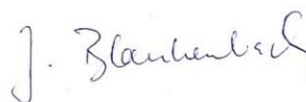
Kind regards,



Phil Bloomer
Executive Director



Gayatri Khandhadai
Head of Technology and
Human Rights



Johannes Blankenbach
Senior EU/Western Europe
Researcher & Representative