Memo

Subject:	**Complainants' responses to NCP questions for final statement in the specific instance SOMO on behalf of 474 Myanmar civil society organisations vs Telenor ASA, in relation to Telenor's irresponsible disengagement from Myanmar**
From:	**SOMO, on behalf of 474 Myanmar civil society organizations (the complainants)**
To:	**Norwegian NCP**
Date:	**31 January 2025**

The complainants wish to thank the NCP for the opportunity to provide this final input on questions posed by the NCP to inform its final statement. What follows are our responses to the NCP questions directed at us. In addition to the below, we have also attached two separate documents related to our proposal for a next step that Telenor could take and our reflections on why the mediation with Telenor failed, as we believe these are relevant to the NCP's questions about what Telenor could have done and still should do to bring its conduct into line with the expectations outlined in the OECD Guidelines for Multinational Enterprises for Responsible Business Conduct.

Due diligence and responsible disengagement

What should be key considerations on responsible entry and disengagement by companies supplying and operating a country's critical infrastructure and telecommunications, particularly in contexts with potential for human rights abuses through government-imposed restrictions and regulations?

The OECD Guidelines and OECD due diligence guidance are very clear that companies operating a country's critical infrastructure and telecommunications, particularly in contexts with potential for human rights abuses through government-imposed restrictions and regulations, should conduct heightened due diligence at both entry and exit, given the heightened risk of severe adverse impacts. Companies in this situation should have a responsible exit plan developed through meaningful consultation with stakeholders and potentially affected rightsholders firmly in place in advance of entry into the market. Companies in this situation should also have a higher than normal commitment to and practice of stakeholder engagement and should be more transparent about their due diligence than in "normal" business situations. As part of their responsible exit plan, companies should be prepared to contribute to the remediation of adverse impacts to which they contributed while operating as well as actual and potential adverse impacts associated with their exit. Telenor

failed miserably in this regard and was woefully unprepared for what was a very clear risk that did end up materializing.

One particular aspect of due diligence that companies entering high risk environments should be aware of in order to not exacerbate risks is not to give customers and rightsholders a false sense of security through marketing and sales pitches. When entering Myanmar, Telenor's public messaging and sales pitch to Burmese consumers it hoped to attract was that they could trust Telenor because the company was aligned with Norway's long-standing democratic traditions, ethical corporate behaviour, and its dedication to human rights and privacy. This marketing scheme convinced millions of customers to sign up for Telenor's services, believing that their data would be safe when that was blatantly not true, exacerbating and compounding the risk to themselves. Telenor Myanmar sought and enjoyed special trust from its customers, who believed their conversations and personal data would be handled safely and securely by a company that marketed itself on its high, Norwegian ethical standards.

In a context of heightened risk due to fragile democratic systems and institutions, business activity in the information and telecommunications sector is particularly risky and calls for extreme diligence and caution. Those who control mobile data wield immense power and possess significant potential for harm. This is particularly sensitive in Myanmar, where users had linked their Facebook accounts and bank accounts, in addition to home addresses, id-numbers, location data and call logs, all linked to Telenor's systems and on Telenor's servers. In addition, the ability of bad actors (including a military junta) to utilize telecoms infrastructure to spy on opponents and root out entire networks adds extra risk to the business, both while operating as well as when disengaging. In this regard, Telenor's sale of its business, including extremely sensitive and valuable user data and surveillance infrastructure, to a company directly linked to the military regime, was a colossal breach of ethics, consumers' trust and of international norms on responsible business conduct such as the OECD Guidelines.

Further, as has been noted elsewhere in relation to challenges to responsible business conduct of companies operating in Myanmar, four different categories of severe human rights impacts can be identified:

1) severe impacts that the sector cannot address;
2) severe impacts that the sector can potentially address;
3) impacts to which companies may be contributing and,
4) impacts that will result from a withdrawal.

It is our understanding that Telenor withdrew from Myanmar based on its understanding that there were severe impacts which it could not address, and which it considered hindered it from meeting international standards on responsible business conduct.

Given the severity of the impacts concerned, complainants understand Telenor's view that it had to disengage, however maintain that Telenor – and all companies considering withdrawing from post/active conflict settings such as Myanmar – should have based this decision on an assessment of the nature and extent of resulting impacts on users' human rights. We note that under international standards on business and human rights, Telenor would have been expected to take into account credible assessments of the potential adverse human rights impacts of a disengagement.

More specifically, in terms of responsible entry and exit, we would recommend a detailed analysis, preferably by a third party with relevant expertise, of:

5) the local context, including at the national and provincial levels, pre-, current, and post-conflict dynamics, value chain due diligence beyond existing sanctions compliance through the integration of local civil society, media, and other watchdog reporting, the national regulatory framework and its alignment with international legal and normative standards;
6) the integration of human rights across national operations, including but not limited to know-your-customer due diligence (with a risk tier-based process for sales), ongoing monitoring of product/service use by local/national value chain partners (including through collaboration with civil society), contractual and technological conditions that, if breached, would result in product/service suspension, and relationships with private military and security companies;
7) "red lines" or risk thresholds that, if crossed, would result in an immediate regular (or heightened in the case of conflict) human rights due diligence process that analysed the ways in which disengagement could impact the local human rights and/or conflict situation (e.g., revenue generation for rights-violating parties, access to personal data, use of infrastructure for attacks against civilians and armed groups);
8) and existing governance mechanisms, board/staff expertise, policies, and other measures that may need to be adjusted based on human rights/conflict risks. The third party analysis would serve as the basis for country strategy or action plan, the non-privileged elements of which should be made publicly available through company reporting and website.

What lessons learned and/or guidance can this case provide for companies considering disengagement in other conflict-affected contexts?

Under guidance by the OECD in relation to business operations in conflict-settings, where the risks and impacts associated with the sector in Myanmar are so significant, companies such as Telenor could reasonably be expected to disengage subject to an assessment of the nature and extent of resulting impacts on users' human rights, and unless the business relationships concerned provide a product or service that is essential to the company's business and for which no reasonable alternative is available. In the event of Telenor, Myanmar is not "essential" to Telenor's business. This means that the most important determinant for exiting Myanmar would have been evaluating whether a responsible exit is possible in light of the human rights impacts of disengagement.

A key question for companies in relation to decisions over exiting a market is the question of leverage. Telenor's perceived lack of leverage with the military has strong implications for due diligence, and companies are unable to mitigate against the human rights impacts perpetrated by the military against Telenor users in the country. Due to the lack of leverage with the military, Telenor considered that it could not handle and address cases pertaining to severe human rights abuses by the military. It is the view of the complainants that, in light of the volatile security context in Myanmar and the military's continued influence and power in Myanmar post-2011, Telenor should have considered risks related to military influence and rule as part of an initial due diligence assessment and decision to enter the country in the first place. Notably, complainants consider that Telenor should have assessed, as part of its initial due diligence, different options of building leverage over the junta. Leverage could have been built, or increased, through various means, alone or in collaboration with other ICT companies engaging in the country. Where risks following military takeover became apparent, Telenor should have re-evaluated prior identified options for leverage and sought ways in which to increase leverage. Similarly, in relation to any due diligence to retract from Myanmar and to transfer operations to new companies, Telenor should have considered what options for leverage – commercial, contractual or other – it had over the buyers, and sought ways to enhance leverage and to exercise it to reduce the risk of harm to the people of Myanmar.

Given the worsening economic and security context in Myanmar that ensued after February 2021, if Telenor would have decided to remain engaged in Myanmar, it should have been better prepared for a responsible exit in the event that it would be forced to leave in the future. Complainants consider that Telenor was not prepared, leading to rash decisions that had real and significant impacts on its users in Myanmar, many of which were being subject to surveillance by the junta for their pro-democracy engagement prior to, and in particular after, the February 2021 coup.

The Telenor example highlights the potential risks to rightsholders and shareholders of not conducting adequate responsible market entry and risk forecasting in fragile, "post"-conflict settings, specifically in terms of: the military's power still being deeply entrenched (by virtue of a constitutional mandate); ongoing ethnic-based conflict (e.g., Kachin State); not immediately and sufficiently addressing law- and rights-violating conduct (e.g., Rohingya genocide) by the "hoped for" democratic government; and not doing sufficient due diligence and corresponding sales decision regarding the exit and sale to M1 Group. In short, hope and reactivity are not good risk prevention and mitigation measures.

In addition, please refer to our previous answer for additional details.

Do you think there are any specific learning points for telecommunications companies in this regard? If so, what are they?

ICT operators should understand, and budget for, the fact that if they have significant activities in a country such as Myanmar, a responsible exit that mitigates the impacts of withdrawal on users will require significant resources and engagement. This should be planned for as a

scenario when initial due diligence is done when entering a market. As part of ongoing due diligence, companies should also re-evaluate their leverage and means to increase it and to exercise it over problematic actors such as the junta. In particular, companies in the ICT sector operating in repressive contexts should be transparent about the means they have to mitigate risks related to user security, and ensure that users understand risks and have ways in which to address those risks.

More specifically, the surveillance-related risks were not properly accounted for, at all, in terms of: the ongoing use before and after the coup of targeted and mass surveillance directed first against personas non grata (e.g., Rohingyas) and then the population writ large; the deficient national regulatory framework and the potential leverage that Telenor and others could use in pursuit of a higher set of international laws and standards; and being overwhelmed by the (foreseeable) speed of events that led to a hasty and irresponsible exit through the sale to M1 Group.

Please also refer to the answer provided for question 1 for additional details.

How can companies in disengagement situations increase their leverage and mitigate risks in collaboration with others?

As we have previously noted, the question of leverage should not first appear in discussions around disengagement, but should be part and parcel of a company's decision to enter a difficult market in the first place. As part of initial engagement, companies should map out, and engage, other companies and entities with influence over difficult actors (such as the Myanmar military) and put in place structures for engagement with those actors. Security aspects related to a potential exit should also be considered at the outset, to prepare companies to exit in ways that do not cause significant risks and harms to users.

As it is used among humanitarian and development actors in fragile and conflict-affected areas, there must be much more coordination between Multinational Corporations (MNC) and civil society organizations operating in these types of markets. Efforts to collectively identify, assess, and mitigate risks, including by industry, could help MNCs better anticipate and respond to human rights, conflict, and material risks. It would also help prevent the "scattering of chickens" effect that takes place when conflict does break out. The growing tolerance (or appetite) for the flouting of international human rights and humanitarian law by state and non-state actors means that MNCs can no longer afford to pursue legal compliance as the only standard by which they do or do not do business with value chain partners. The scope, depth, and breadth of their value chain due diligence needs to reflect each state's (or province's) level of conflict, fragility, and corruption.

More specifically, the OECD Guidelines and OECD due diligence guidance also contains many clear recommendations and suggestions for how companies can use leverage and mitigate risks in disengagement situations.

1. Front-load leverage by being prepared and carry out risk-based due diligence as part of its decision-making process surrounding a potential exit. This includes establishing a mechanism and procedure to properly identify risks and impacts (including those associated with the disengagement itself) and the company's relationship to them and what that implies for the company's due diligence and responsible business conduct.
2. Engage meaningfully with stakeholders and in particular potentially impacted rightsholders and their chosen representatives in the decision to exit
3. Provide maximum transparency surrounding disengagement decision-making, particularly towards rightsholders, but also toward other companies who might be facing the same problems. If certain disclosures pose safety or legal risks, companies should seek to find creative ways to enable crucial information to get to rightsholders.
4. Collaborate with business partners, other companies, and relevant stakeholders to remediate harms committed or contributed to while operating and to mitigate ongoing potential risks associated with the disengagement. We have proposed very concrete models for this to Telenor.

What could responsible disengagement look like in the context of the present case?

Telenor should have adequately assessed the human rights impacts in accordance with principles 19 and 24 of the UN Guiding Principles. If the findings show that the sale to a specific buyer would cause or contribute to harm to rightsholders, then the company should either not proceed with the sale or address how it plans to mitigate or prevent such harm from taking place. We have also made additional recommendations in the answer provided for question 1, recommending the involvement of a third party with relevant expertise. Responsible disengagement in the context of the present case should have included strong human rights due diligence in relation to the sale. This due diligence should have happened before the sale went ahead and the data was transferred to the buyers. This should have included an assessment of the risks of transferring the historical metadata and current user data to the buyers: M1 Group and Shwe Byain Phyu, particularly in light of these companies' business operations and ethical behaviour elsewhere. Human rights due diligence should have entailed meaningful engagement with potentially impacted stakeholders and should have identified preventative (and if prevention was not possible, mitigation) actions that should be pursued. These actions should have corresponded to the likelihood of negative human rights impacts occurring, and their impact should these occur.

In this case, it remains unclear how Telenor carried out a human rights risk assessment and due diligence, if any, and how the company concluded that selling to M1 Group and ultimately Shwe Byain Phyu was the least detrimental option. As the complainants have shown, Shwe Byain Phyu is a company known to be closely linked to the Myanmar military. The direct consequence of this is that the company would likely share all sensitive user information with the military. In addition, Telenor has built its business model in Myanmar around the respect for human rights and democracy, making itself as the only "trusted" network in the country.

Therefore, this comes with additional responsibility to protect the trust of customers placed in Telenor and ensure that any exit is done with high due-diligence and accountability, and respect for the customers' rights.

Telenor's due diligence process in relation to the sale specifically should have assessed:

- Full know-your-customer due diligence process to assess the current buyer's policies and practices on human rights, including history of human rights track record, as well as capacity and competence of the buyer to manage and operate responsibly telecom infrastructure. Any KYC should have been backed up by a third-party assessment.
- A full assessment of other potential buyers at the country and regional levels, using the same KYC approach.
- Risks related to how M1 Group and Shwe Byain Phyu would handle user data, the likelihood of these companies transferring this data to the military, and the impacts on Myanmar citizens, in particular opponents to the military takeover, should the data be shared.
- Options to prevent, and if prevention was not possible, to mitigate adverse impacts related to a potential sale. These options should have been identified prior to any engagement with potential buyers, and should have been adapted to the de facto buyers and risks associated with them and their connections to the military. Telenor should have sought to create leverage (or sought to increase existing leverage) as part of any business deals, including with the Myanmar government once the company entered the market in the first place, and with the de facto buyers. Contractual clauses would have been one means of increasing/exercising leverage. For instance, if these conditions are broken, then the buyer would face financial penalties or network suspensions, or contract could have included a transition period to ensure that these guarantees are met, and if not, breach of contract would have led to the suspension of the asset transfer.
- Being transparent, at the outset and when entering the market, about any legal basis for preserving all data of subscribers and transferring this data to the buyer. It remains unclear to complainants on what legal grounds Telenor was required to retain all customer metadata (for instance, was this an order by the junta, a statute, or a contractual requirement?). It is the view of the complainants that Telenor knew, or should have known, that certain types of metadata should have been excluded from any legal or other "requirement" to retain metadata.
- Identification of options, and implementation of these, to minimize the amount of data that was transferred to the buyers in the first place. In particular, it is the complainants' view that Telenor should have amended the terms of the sale to exclude the transfer of customer/user metadata to the buyer i.e., to restructure the transaction in order to ensure that the buyer receives Telenor's physical assets (e.g., phone towers and various other physical infrastructure) but does not have access to any user metadata. Telenor could have also explored other technical measures to protect user data, such as encrypting or anonymizing sensitive user data before the transfer, ensuring that even if user data is transferred, it could not be easily accessed or linked to individual users.

In addition:

- Risks related to the sale could have been mitigated, to some extent, if Telenor had informed users about risks to their security and possible steps they could take to mitigate these risks. Telenor should have taken proactive measures to directly reach each of its users to inform them of their risks post-sale and provided clear recommendations on how they could protect themselves. Telenor could also have collaborated with digital rights groups to provide trainings to high-risk individuals to minimize their risks post-sale. Many users, including civil society activists, did not, and still do not, know the content of the data that has been collected by Telenor. This lack of clarity makes it difficult for them assess their levels of risk following the data transfer. Telenor should have explored funding mechanisms to provide material and technical support to users to help mitigate risks to them following the sale of their user data. If risk mitigation plans of this sort were not feasible, Telenor could have explored the option of staying in Myanmar, without operating in the country, until the number of years required before it could delete historical user data had been reached.
- Importantly, as part of any internal discussion and due diligence on its sale, Telenor should have carried out stakeholder engagement with Myanmar stakeholders. Telenor wrote off the value of Telenor Myanmar in early May, one month before the sale to M1 was publicly announced, meaning that the company had at least one month to consult stakeholders. Telenor should have stated publicly that they are considering divestment to allow for such consultations, as this would not have had significant impact on their share prices since they had already written off their investment.

Risk mitigation and remedy

What can be appropriate remedy mechanisms and remediation for handling negative impacts related to telecommunications companies disengaging from conflict-affected areas?

Meaningful engagement with diverse stakeholders can help the company explore options for companies to mitigate risks to users and to identify, together, ways to work together, and as relevant also in collaboration with others, to seek to mitigate the adverse impacts of disengagement. This requires the company to be transparent about risks to users stemming from a potential engagement and working with stakeholders to mitigate those risks, including, as relevant through financial and material support, prior to exiting the market/disengaging.

What would be a reasonable role for Telenor to play in terms of risk mitigation and remedy when disengaging from Myanmar, both by financial and non-financial means? Alone and/or jointly with other actors?

To abide by the OECD Guidelines, we expect Telenor to:

- be more transparent, particularly as severe human rights impacts were highly likely in Myanmar;
- meaningfully engage with rightsholders on crucial decisions including disengagement and to do so prior to a decision being made;
- publicly acknowledge that Telenor's decision to exit without stakeholder input led to harm to users in Myanmar;
- provide and facilitate access to remedy for Myanmar users (victims of impacts to which Telenor has contributed); and
- provide training for civil society members regarding digital security measures that they should start implementing in response to the risks that they may face following Telenor's transfer of their data to military-linked business entities. An information campaign of some sort could be helpful to consider and to reach former users that may still be unaware of the risks they take.

What role could a digital security relief mechanism, based on recommendations in the Myanmar ICT Ecosystem Study, play in this case; what is required for it to become reality, how could it be governed and how could any risks arising from such a mechanism be mitigated?

The ICT Ecosystem Study was limited in terms of details of the digital security relief mechanism. This is the reason for which complainants agreed to wait until the final mediation round to expand on the digital relief mechanism.

To expand on a potential digital relief mechanism that would be impactful and valuable to users at risk in Myanmar, complainants carried out a consultation with civil society actors from diverse states and regions in Myanmar. During these consultations, we reached a preliminary agreement on the initial objectives and design of a potential digital relief mechanism, including that the overall aim of the Mechanism should be to contribute to the digital safety and independence of pro-democracy actors, and broadly strive to enhance the resilience and sustainability of local societies to protect communities from adverse impacts caused by the Myanmar junta through digital technological support.

In particular, a Mechanism could support the development of decentralised digital infrastructure managed and overseen by local civil society actors in collaboration with local governance actors that have arisen following the coup. Given the significant risks associated with the Myanmar junta's surveillance technologies and connectivity barriers following widespread internet and mobile shutdown, local actors in each state and region have initiated creative and adaptive strategies to address and overcome key security and connectivity issues. However, technical and financial resources are needed to improve and expand these initiatives. Developing the infrastructure adapted to the crisis context would enhance local civil society and governance actors' ability to provide critical services to the communities, including in health, education and addressing humanitarian needs. The development of the infrastructure would require an initial in-depth technical assessment of the feasibility of

utilising and expanding cross-border digital networks in areas of Myanmar that border with India, China, and Thailand, restoring damaged fibre cables, and expanding Starlink networks. Telenor's expertise and experience of the digital eco-system would be valuable for assessing realistic infrastructure options and networks and its associated risks and would support the implementation of action (a) agreed in the Memorandum. This would be aligned with the ICT ecosystem sector report's recommendations for potentially supporting safe and reliable communication networks. In particular, the study made a recommendation to all ICT companies to identify ways that they could support digital safety and security of users, including supporting initiatives to build digital safety and security understanding amongst users, providing financial and material support, and offering services and features to support their safety and security.

The relief mechanism could also support the digital security of Myanmar citizens by funding existing or developing safe alternative forms of communication, providing VPN access, and emergency grants. This was mentioned in the ICT ecosystem sector report as tangible potential areas of support. The study defined a digital relief mechanism as "understood to mean a fund of some kind, focused on reducing risks relating to digital footprints for people in Myanmar, including offering support to activists, HRDs and the general population". In addition, recommendations included supporting technical tools such as VPNs, funding for safe houses, and supporting safe and reliable communication networks, in addition to resources to support the work of HRDs inside and outside the country.

The mechanism could be managed and overseen by a consortium of international and local organisations to govern and address potential risks that arise.

What would be a possible way to identify and remedy any harm to employees after a telecommunications company has disengaged from a country due to unacceptable human rights risks related to its operations?

Set up a **digital security relief mechanism** that employees and former employees feel safe using.

Forward looking recommendations and follow-up

What should be key action points moving forward from where the specific instance stands now, also in relation to continued follow-up of the MoU?

It is clear that Telenor must take action to bring its conduct in line with the OECD Guidelines. As a first next step, Telenor should finally acknowledge and take responsibility for the fact that it contributed to severe adverse impacts during its time of operation in Myanmar through the collection and transfer of sensitive personal information of its customers to the military junta, and that it contributed to severe actual and potential negative impacts through its disengagement from Myanmar. Following from this (and from the expectations outlined in the Guidelines for a company that has contributed to adverse actual and potential impacts),

Telenor should take action to contribute to the remediation of the adverse impact and to the mitigation of ongoing risks to which Telenor contributed through its disengagement. Telenor should finally begin meaningfully engaging stakeholders and especially rightsholders in this effort. As for what this mechanism or effort should be, we have previously proposed a Myanmar Digital Resilience Mechanism, that reflects the forward-looking, risk prevention and mitigation nature of what is so urgently needed to protect Telenor's former customers in Myanmar following Telenor's exit. Although Telenor previously dismissed our proposal outright, we believe it is still a valid proposal to consider, at least as a starting point.

The Norwegian government, as a majority shareholder in Telenor, also has a duty and a responsibility to take action in this regard.

Regarding the mediation process, Telenor has not meaningfully engaged, failing to demonstrate transparency or even a genuine interest in dialogue. The information it has shared during the process was already publicly available on its website, with no real effort to engage openly or associate with civil society groups. Although an MOU with a limited scope was agreed upon in the hope of advancing discussions, no tangible progress has been made. Instead, Telenor has attempted to bypass the mediation entirely, cancelling sessions at the last minute and disregarding civil society groups in the process. Given this, Telenor must now acknowledge the harm caused by its actions, take responsibility, and conduct a genuine and thorough investigation into the events that transpired and the harm resulting from its disengagement.

What progress should be expected within one year?

Myanmar civil society organizations believe that Telenor has completely disregarded the mediation process and the legitimate concerns outlined in the MOU, instead attempting to bypass mediation and bury the issue. To regain the confidence of civil society groups, Telenor must engage meaningfully in the mediation and demonstrate a genuine commitment to making it work. It should also make a public announcement of and substantial progress on implementing the digital security relief mechanism.