Telenor ASA
Snarøyveien 30
N 1360 Fornebu

Norges kontaktpunkt for ansvarlig næringsliv
Pb 8114
N 0032 Oslo

Date
20/01/2025

Organisation number
982463718

Letter sent by email only

Telenor's forced exit from Myanmar

1 Introduction

We refer to the Norwegian OECD Contact Point's (NCP) email 31 October 2024. Telenor will in the following provide answers to the NCP's questions. Questions 1 to 4 are answered in section 2 and the remaining items are addressed in section 3.

The Telenor Group's (Telenor) forced exit from Myanmar took place in exceptional circumstances. Telenor's risk assessments, stakeholder dialogue and mitigation actions, including on human rights, is best understood in the context of how the situation in Myanmar unfolded, and the options available to Telenor. We will thus answer NCP's question 1 to 4 mainly based on the sequence of the events.

The NCP has asked not to receive information that needs to be kept confidential. Risk assessments during the exit process, including on human rights, were conducted using both internal resources and external expertise. Some of the input for these assessments came from sources within Myanmar. The security situation in Myanmar remains challenging, with a significant risk that the military regime could retaliate against such sources. Furthermore, the external experts have requested that their reports are not shared externally due to concern for people safety. Telenor will thus not provide information that could compromise anyone's security, is confidential due to agreements with third parties, or that otherwise contains business secrets.

While Telenor will attempt to balance the need for confidentiality with our commitment to transparency our response is thus limited to information that can be made public. This also means that Telenor will only to a limited extent be able to provide copies of assessments made after the military coup in February 2021.

2 Question # 1 to 4

2.1 Telenor Group's policies (Question #1)

Telenor's Code of Conduct set the overall standard for human rights for Telenor. The Code of Conduct is approved by the Telenor ASA Board of Directors, and all employees yearly commit to understanding and complying with the Code of Conduct.

https://www.telenor.com/about/corporate-governance/code-of-conduct/

It should be noted that up until 2023 Telenor did not make internal policies available outside of Telenor. There were also additional changes to the governance framework in 2023. However, the governance and policy on human rights has not been changed significantly. As shown in the *Group Policy Sustainability,* Telenor employs an ongoing process of human rights due diligence to identify, prevent, mitigate and account for how to address human rights impacts.

https://www.telenor.com/binaries/about/public-policy/Group-Policy-Sustainability-web-version.pdf

Key to Telenor's efforts with respect to human rights are:

- Policy, tools and training to build capacity in Telenor companies
- Stakeholder engagement internationally and locally, including in Myanmar while we had operations there
- Transparency and public reporting

Telenor has implemented a *Human Rights Due Diligence Toolkit*. It addresses how Telenor and its subsidiaries work to identify, prevent, mitigate and account for human rights risks and impacts resulting from its own activities and value chain.

Grievances can be reported by anyone through Telenor's Integrity Hotline. Telenor's *Supplier Conduct Principles* include provisions on human rights which all suppliers must adhere to.

2.2 Pre-coup human rights due diligence (Question #1)

Before entering Myanmar, Telenor conducted its own due diligence and commissioned several third-party pre-investment due diligence processes, including on corporate responsibility risks and opportunities. This covered human rights, labour rights, corruption and environmental sustainability. As part of this effort Telenor engaged third parties including BSR (Business for Social Responsibility).

BSR is a leading non-profit focused on corporate sustainability since 1992, with expertise working with business on a wide range of issues associated with the environment, human rights, economic development, governance and accountability. BSR's conclusion, was that Myanmar was "*on a positive trajectory towards increasing economic and political reform and that the country was in the early stages of a nation-building process.*"

https://www.bsr.org/en/case-studies/telenor-responsible-decision-making-in-myanmar#:~:text=In%20order%20to%20understand%20the%20potential%20sustainability%20risks,human%20rights%2C%20labor%20rights%2C%20corruption%2C%20and%20environmental%20sustainability

In 2020 Telenor commissioned an extensive assessment by Article One of human rights risk in Myanmar. Article One is a specialised strategy and management consultancy with expertise in human rights, responsible innovation, and sustainability. The report was delivered to Telenor in January 2021. While work was underway to assess how to work with the findings the military seized power in a violent coup. The Article One report has been shared with the NCP previously.

In Telenor's communication with the NCP in the matter 'Committee Seeking Justice for Alethankyaw (CSJA) vs. Telenor', human rights due diligence, stakeholder engagements and mitigating activities during the pre-investment and operational phase is described in more detail.

With respect to the current matter before the NCP, it is appropriate to include additional information regarding Authority Requests (AR). In general, all countries require telecommunication authorities to comply with different requests. Such requests can include, e.g., blocking of URLs, shutdown of networks, distribution of government information and access to historical data. Lawful Intercept (LI) is a form of AR. LI covers real-time interception (i.e. wire-tapping, positioning for emergency situations, etc.), and access to content of communications, traffic data and location information, i.e. access to information on the location of mobile terminals/phones. Further information on AR and how Telenor handles these can be found at Telenor's website:

https://www.telenor.com/esg/governance/handling-access-requests-from-authorities/.

While LI is necessary to solve crimes, prevent security threats, or find missing persons it also represents a risk to privacy and freedom of expression. Telenor identified this as a human rights risk before a bid for a license was made. Telenor therefore entered the Myanmar market on the clear understanding that the legal framework for LI would be based on international best practices, with proper checks and balances in place (such as court orders for LI requests) and that LI would only

be used in a manner that was consistent with the Myanmar Constitution and that respected fundamental rights. This was what Myanmar had committed to during the bidding process and TML continued to reiterate this with the authorities.

During the period Telenor operated in Myanmar we refused to activate LI until adequate safeguards were established and maintained a continuous dialogue with the civil authorities in Myanmar. This effort included advocating for a legal and regulatory framework for LI in line with international best practices. In 2018, the EU and Norway imposed sanctions on LI equipment. Facilitating LI without proper safeguards would violate international human rights standards and sanctions, conflicting with Telenor Group's core values as a company. The LI equipment was not activated while Telenor remained in Myanmar.

2.3 Human rights considerations in dramatically changed circumstances following the coup (Question #1 and #2)

Around 2am on the day of the coup 1 February 2021, armed personnel from the Tatmadaw forcefully entered Telenor Myanmar's (TML) data centres.. The situation was tense and disorderly. TML's data centre in Mandalay was ransacked, and the power for the IT racks and virtual core nodes were shut down improperly, with the wires and cables of the IT racks and fire-fighting systems forcefully ripped out by armed personnel.

The coup changed the situation in Myanmar in a dramatic manner. Telenor and TML had to transition from dealing with a civil authority to dealing with a military regime with powers subject to minimal legal constraints. The military regime introduced martial law in defined areas in Myanmar mid-March 2021, as well as a new extensive cyber security law with limited legal safeguards. Telenor publicly protested against the cyber security law, citing human rights as a key concern. In this difficult situation TML had to comply with local laws while at the same time seeking to honour human rights principles and standards to the extent possible under Myanmar law.

Telenor established a crisis organisation and framework to manage the situation. A steering committee (SC), led by the then EVP and Head of Telenor Asia, was responsible for daily crisis management and met frequently until Telenor Group safely exited Myanmar. The crisis organisation consisted of various internal experts, including sustainability and human rights experts.

One of the SC's first task was to assess risk and prioritise mitigating actions. The first and initial risk picture was established during the second week of February. This included human rights. It was at this point evident that risk assessments conducted before the coup had limited relevance. By the end of February, follow up discussions were conducted with relevant internal expert functions and external

experts. These discussions informed the mitigating activities, and the establishment of a common risk understanding within Telenor management.

A full review of mitigation measures and residual risk after implementation of mitigation measures was decided by the SC in mid-March 2021. It was, furthermore, decided to integrate human rights risk, including risk to employees, customers and other stakeholders, into the overall and operational crisis management. It was Telenor's view, that human rights due diligence should not be managed as a standalone issue but should be an integrated part of the crisis handling.

Early March 2021 the SC, based on an assessment of risk and areas where Telenor would be able to mitigate, decided to prioritise the following:

(i) First and foremost, ensure personnel safety and security.
(ii) Ensure continued network availability for the customers.
(iii) Stay transparent to the extent possible when handling orders from the military and on the developments on the ground in Myanmar.
(iv) Safeguard the operations.

In addition, Telenor decided that it would not activate LI. The military regime exercised considerable pressure on Telenor to comply with its demands to activate the equipment. However, Telenor did not activate the equipment.

Telenor's human rights commitment was a key factor in prioritising these risks. The heightened risk of human rights violations in a conflict affected country such as Myanmar was duly acknowledged in the risk assessment and prioritisation. While Telenor employs recognised methods and processes for managing risk (assessment, development and implementation of mitigating actions and subsequent monitoring of actions and results) this is not always feasible to follow in a linear way in a crisis. Events, both foreseen and unforeseen, impacted what Telenor could and should do during the forced exit from Myanmar.

Firstly, protecting the life and health of employees is a requirement under international human rights standards. As part of this, TML local employees were instructed not to oppose orders from the military regime if they felt their safety and/or life was in danger, as it was clear that this could entail severe consequences for the employees. At the same time the TML management opposed the orders to activate LI.

Secondly, ensuring that TML's customers could use TML's mobile network made it possible for people in Myanmar to communicate and access information, thereby also exercising their right to freedom of speech through, e.g., use of VPN and

access to encrypted services such as Signal or WhatsApp. When the military regime ordered the internet blocked, TML offered subsidised voice call and SMS packages for customers in the absence of mobile internet services. TML also informed customers about how to use the internet safely. It was our clear impression that many people in Myanmar started using VPN and encrypted services.

In addition to communication access, physical safety remained important. As the violence increased in Myanmar many of the telecom tower sites were sabotaged and vandalised, and the military regime placed anti-personnel landmines around them. TML engaged with community leaders to inform their communities to stay away from the tower sites, broadcasting SMS alerts to customers who lived near unsafe tower sites and conducted mine awareness training through an external mine expert to relevant TML and vendor employees.

Thirdly, to help defend the customers' right to privacy, Telenor was transparent on authority requests on its website. Since the coup Telenor published each request, until the military regime forced us to discontinue the practice. Telenor was transparent on that we could no longer publish authority requests. We, furthermore, expressed grave concern with this development not allowing transparency and recognised the impact this had on the local and international community's ability to receive information. Telenor still continued to be as transparent as possible, and all statements and the overview of orders received can be found here:

https://www.telenor.com/esg/social/human-rights-in-myanmar/directives-from-authorities-in-myanmar-february-2021/

Telenor also spoke to international and local press, including on the intent of the military authorities to activate LI. Transparency and providing as much information as possible to the people of Myanmar and the international community were important values we strived to uphold. However, the priorities did sometimes conflict, and the safety of our employees remained a prime responsibility.

2.4 Assessment of all exit alternatives and human rights consequences (Question #1)

Soon after the coup the military authorities exerted significant pressure on Telenor to activate LI. Telenor refused to do so, which resulted in key foreign personnel being denied exit from Myanmar. It was clear to us that complying with such orders from the military regime would have had a high human rights risks/impacts. Under the UNGP a heightened due diligence is required when operating in conflict-affected and high-risk areas, and human rights were assessed as an ongoing risk in the period. With martial law in place and all civilian protection of rule of law disbanded, the threat to our employees, both local and foreign, was substantial.

The situation left Telenor with no other options than to exit Myanmar. It would not have been possible to continue operating in the country without activating LI, as the standing order from the military regime was for all telco operators to activate the system.

The steering committee developed possible exit alternatives for Telenor, with thorough assessments for each scenario, as it remained unclear what exit route would be feasible, and all options needed examination. The alternatives were to surrender the licence, to abandon the operations or to sell TML.

Licence surrender would not have been accepted by the military. This would have left Telenor in a deadlocked situation which would have made an orderly exit impossible.

The assessment of immediate abandonment of the operations showed increased human rights risk to our employees, including loss of livelihood. The risk also increased for all local workers in the wider supply chain, as they would also lose income in a country on the brink of civil war. Furthermore, there was a high risk of retaliation towards our employees from the military, such as imprisonment and even risk to lives. In addition, the network would be shut down and all maintenance halted, where Telenor could not guarantee for environmental damages.

Destruction of TML's customer data was properly assessed, but the time frame to execute would have been so limited that the exercise would be almost futile. It would also significantly increased the risk of physical harm to our employees. Finally, in both the licence surrender and abandonment scenarios we would not have been able to get our foreign employees safely out of the country.

While HuRi assessments were an integrated part of the crisis management work, a separate HuRi assessment was developed for the immediate abandonment scenario as this was seen as a scenario with risks for severe and broad negative impacts on human rights, including health and safety and life of employees.

The human rights due diligence of this scenario is enclosed as

Attachment 1: Telenor Human Rights Impact Assessment

The military made it clear that they wanted a sale and continued operations of the network in Myanmar, and the exit choice was thus forced. It was the option that was the least detrimental and which would best safeguard the people Telenor had a primary responsibility for, our employees. In addition, it would ensure a continued fourth network in Myanmar, supporting communication for the Myanmar people.

2.5 Decision to sell and sales process (Question #3 and 4)

Sale was in an overall assessment, including the human rights aspects, the least detrimental option in a situation with no good options. A sale would entail continued jobs for Telenor Myanmar employees, continuation of TML's communication network in the country, and continued income for partners and supply chain in Myanmar. It would also prevent any retaliation towards employees, and was the only route where Telenor could get guarantees that foreign employees would be permitted to leave the country.

However, the military coup caused significant unpredictability, volatility and severe human rights and security challenges, which barred us from conducting an extensive and prolonged sales process. There were limited numbers of potential buyers, also since LI in Myanmar were subject to EU sanctions. In addition, the military regime had set a fixed deadline for activation of LI, which Telenor could not comply with. We conducted an Integrity Due Diligence on all potential buyers and chose M1 Group (M1) since it was an international buyer with significant experience in telecommunication and a long-term intent for Myanmar.

Human rights including privacy were key considerations during the sales assessment. However, it is important to note that no operator would be in a position to continue denying activation of LI under the military regime, without severe human rights consequences to its employees. Financial considerations were not important. In fact, Telenor suffered a significant financial loss with the sale of TML. For M1 Group, the transaction was fully self-funded in that there was cash left in TML's bank accounts in Myanmar that was greater than the amount of money Telenor received for the sale.

Due to the military regime's continued LI pressure, and Telenor's refusal to activate, and the consequential risk to our employees, the sales process was concluded quickly. Telenor conducted a holistic risk assessment, including human rights impact assessments and sustainability assessments, in connection with the sale of TML. However, these assessments were intertwined with internal communications and other considerations and sharing externally – even today - would increase people security risks. In Telenor's extensive learning after closing of the sale process, please see below for more details, one lesson learned was that such assessments should be documented as standalone so that they can more easily be shared with specific external stakeholders. The lessons learned, which included involvement of civil society organisations, can be found here:

https://www.telenor.com/esg/social/human-rights-in-myanmar/myanmar/outcomes-of-telenors-internal-learning-process-from-the-myanmar-engagement/

Sometime before closing of the transaction with M1, Telenor was made aware that it would be a requirement from the military regime for M1 to have a local partner once the transaction had been completed. Telenor did not take part in the dialogue with the authorities on this. We were also made aware of plans between M1 Group and Shwe Bin Phyu (SBP) for a potential transaction after the closing of the deal between M1 and Telenor.

Before closing the sales transaction, Telenor Group conducted meetings to discuss human rights best practices with M1 Group and encouraged upholding international best practice standards for the company in Myanmar (today branded as "Atom"). After the sale Telenor has maintained agreements to ensure that people in Myanmar are able to communicate with the outside world.

Attachment 2: Responsible Business in Myanmar, Presentation to M1

Telenor sold TML wholly to M1 Group. Due to the information of the potential transaction between M1 and SBP, Telenor conducted an IDD on SBP, including human rights and sanction issues, which did not change our assessment that a sale was our only option, nor did it change the human rights assessment of the transaction significantly.

When it comes to privacy issues and activation of LI, any owner would have to comply with the local legal requirements for authority requests. The sale did therefore not change the risk to the customers' privacy. Today, M1 Group is still a co-owner of Atom and is actively involved in the operations of the company.

2.6 Employees in TML (Question #2, 3 and 4)

To ensure people safety TML set up a system with daily contact with each employee to ensure all were accounted for, and this was a reporting point in each SC meeting. TML, in dialogue with Telenor Group, had a high frequency on communication to employees. In TML there were regular "town halls" and Q&A sessions with the company's CEOs. The principle was that the employees should be the first to be made aware of developments.

When the sale was announced employees in Myanmar were informed at the same time. Regular communication was maintained during the transition period and closing of the sale, and Telenor invited M1 in to speak to employees so that they could hear directly from M1 about their plans for further operations of TML. To Telenor it was important to keep employees well informed, so that they had ample time to make the right choices for themselves.

In connection with the sale Telenor secured benefits for the employees. This included salary increment and payment of bonuses. Some were paid before closing

and some were eligible after handover to M1. Some employees who had roles entailing a perceived high risk were given options outside of Myanmar in other parts of Telenor.

However, it is important to note that it is not common practice in any business to discuss the sale of the company with the employees, as that dialogue remains sensitive and confidential until it is concluded. In this situation we had the added responsibility of keeping employees safe and the situation was unpredictable and volatile. Therefore, any broad TML employee consultation, beyond key personnel who were working to prepare for a transaction, would not be feasible and was not conducted.

It should be noted here that in addition to the coup the Covid pandemic was at its highest during this period. TML implemented several mitigating measures, such as vaccinations to ensure the safety and wellbeing of TML employees.

2.7 Dialogue with stakeholders (Question # 1 to 4)

Throughout Telenor's operations in Myanmar, we had extensive dialogue with stakeholders. In 2021 there were at least 125 different calls/meetings concerning the human rights situation in Myanmar. Until June 2022 there were at least 36 calls/meetings. The different stakeholders included civil society organisations within and outside of Myanmar, investors and authorities. Telenor provided as much information as possible, discussed dilemmas and received valuable input which was utilised in Telenor's human rights due diligence and mitigation.

Telenor also provided extensive information in the public domain during the period. Please find attached an overview of facts available in the public domain compiled by the mediators.

Attachment 3: Overview of facts available in the public domain compiled by the mediators

3 NCP question # 5 to 15

3.1 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? (Question #5)

A responsible entry should include human rights due diligence as defined in the UNGPs and the OECD Guidelines for Multinational Enterprises on Responsible

Business Conduct. It should be noted here that while each country and time is different, not only human rights but also the level of local corruption and extent of rule of law might present different impacts, risks and opportunities. And those may evolve over time. Telenor conducted a thorough human right due diligence when entering Myanmar.

Following responsible entry, active ownership is core. In this context, active ownership includes strong commitments from top management to international human rights standards and anti-corruption. These commitments should be communicated both internally and externally. Internally through active and maintained dialogue and joint decision-making between headquarter and local company, based on local training and understanding of policy commitments and processes. External transparency should include not only the human rights commitments, but also, as far as possible, both achievements and challenges. External stakeholder dialogues should include local stakeholders.

The learnings with regards to impacts, risks and opportunities in this case are based on the fact that Telenor's disengagement was forced by the military junta, and that the exit was performed under crisis management. The same key considerations as for entry and active ownership apply as a starting point. Due diligence should include due diligence of the buyer. Post-sale, the seller should seek to transfer knowledge of human rights impacts, risks and opportunities as well as policies and procedures to the new owner. In conflict-affected and high-risk areas the seller should provide options for at-risk employees. Telenor implemented these measures.

Considerations specific to telecom operators—also based on the case of Telenor's forced exit from Myanmar—include being as transparent, as detailed and timely as possible, about specific authority requests on network shutdowns and surveillance related requests. A telecom operator should seek to uphold dialogues with local decision-makers and stakeholders on telecoms and internet regulatory reform in support of the rule of law and of economic development.

3.2 What lessons learned and/or guidance can this case provide for companies considering disengagement in other conflict-affected contexts? (Question #6)

As set out above, Telenor provided regular public updates on e.g., the risks faced by its employees and the people in Myanmar, the requests it was receiving from the military as to network shutdowns, the decision to sell the company, and the sales process. This information, as well as additional information related to Telenor's operations in Myanmar, can be found here:

https://www.telenor.com/esg/social/human-rights-in-myanmar/myanmar/

Please also see attachment 3.

In 2023, Telenor published a set of learnings from its process of engagement and disengagement from Myanmar, please see the link above.

The report, supported by law firm Wikborg Rein, includes input and reflections from civil society organisations. Key lessons learned were the following:

Lesson #1 – New risk-based approach to crisis management: The risk-based crisis management process adopted by the Steering Committee – which involved defining priorities based on risk, with quality assurance from external and internal contributors – was highly successful and should be followed in future crisis situations. The early identification of people safety as a key priority governing crisis management is an example of this approach being successfully applied in practice.

Context: From the outset, the SC based its decision-making on a holistic and continuously updated risk assessment, grounded in input from all relevant internal functions, as well as external experts. This ensured an effective and well-reasoned decision-making process based on a wide appreciation of relevant risks, which was carried through all the way up to the Telenor ASA Board of Directors.

Lesson #2 – Crisis preparedness: Telenor's standard processes for entering new markets could usefully include discussions around business continuity (including putting in place evacuation protocols) and considerations relating to a responsible exit. Such discussions might subsequently facilitate prompt decision-making during a crisis.

Context: There seems to have been limited pre-crisis focus on potential exit options and staff evacuation scenarios. Although the extent to which this would have made a difference in practice is not clear, responsible exit considerations are fast becoming part of best practice principles expected of large organisations such as Telenor and could usefully be embedded in the organisation.

Lesson #3 – Internal information flows: In a future crisis, more consideration should be given to ensuring that top management representatives with functional responsibility communicate more effectively to their respective expert level reports to foster understanding of and trust in the decision-making process among all contributors.

Context: Capacity and confidentiality constraints limited the flow of information from the top down, resulting in a lack of understanding of, and, for some, a lack of faith in, the crisis decision-making process. This lack of understanding/faith seems,

however, to have been based on incomplete insight into the decision-making process, as all relevant expert functions were represented at Steering Committee level. It could likely have been remedied through more effective communication about the well-informed, risk-based nature of the decision-making processes of the Steering Committee and Telenor ASA Board of Directors.

Lesson #4 – NGO/CSO stakeholder dialogue: In a situation where stakeholder dialogue with and transparency towards NGOs and other civil society organisations (CSOs) are tempered by confidentiality constraints, Telenor should strive to share as much information as possible with teams responsible for dialogue with such stakeholders (this also applies to other stakeholders where information could end up in the public domain). This may equip relevant teams with the tools to engage in a more nuanced dialogue, with the aim of mitigating the risk that NGO/CSO stakeholders perceive Telenor's communications as deliberately misleading. This lesson does not apply to dialogue with other stakeholders, which generally appears to have been well received.

Context: There is widespread sentiment within certain teams that a lack of internal information sharing resulted in misunderstandings and miscommunications in dialogue with NGO/CSO stakeholders, with ensuing negative consequences for Telenor’s reputation and standing. In contrast, communication with various other stakeholders, such as public authorities, politicians and Telenor's owners, seem to have been successful.

Lesson #5 – Human rights risk assessment: When conducting human rights and sustainability risk assessments within the context of a wider risk assessment (e.g., in a crisis), such assessments should be documented as standalone so that they can more easily be shared with specific external stakeholders such as NGOs, which tend to focus more singularly on human rights and sustainability considerations.

Context: Although Telenor conducted a holistic (360) risk assessment, including human rights impact assessments and sustainability assessments, in connection with its various options for exiting Myanmar, these assessments were intertwined with internal communications and other considerations and sharing externally would have resulted in increased people security risks. This resulted in a perception

– and subsequent criticism of Telenor – among some stakeholders that Telenor had not conducted a human rights risk assessment in connection with the sale.

Lesson #6 – Crisis management procedures: Telenor's risk-based crisis management approach departed from existing written procedures but worked well and would be adaptable in future crisis situations. Existing procedural documents for crisis management should be updated to reflect this new, dynamic approach.

Context: The coup revealed that Telenor's existing (pre-coup) crisis management procedures were not fully fit for purpose (i.e., were not especially useful in the context of the coup). In practice, this was alleviated by Telenor's dynamic approach to crisis management (as described in lesson # 1). Codifying this in writing can ensure a similarly adaptable approach becomes Telenor's new procedural norm for crisis management.

It should be noted, in case sanctions apply, the constraints such can put on a company seeking the best way forward for the company, its employees, and its customers to exit. Also, different human rights commitments and considerations can be incongruent. In the case of Telenor and Myanmar, employees were, by the military, put in the highest risk perceivable. As an example of a mitigating activity following up the risks to employees, management counted each employee each day.

3.3 Do you think there are any specific learning points for telecommunications companies in this regard? If so, what are they? (Question #7)

The learnings identified apply generally, not only to telecommunications companies. See answer to question 6 above.

It should be noted here that Telenor Myanmar was one of many players in the digital eco-system in the country and the data associated with its services made part of a wider users' digital footprint. This fact was not known to all stakeholders, including users, CSOs, and policymakers. The parties thus, as part of the MoU, agreed to commission and 'Independent ICT Eco-system Study', (the ICT Study).

According to the public MoU, the parties agreed for Telenor to *"support the complainants in enhancing Myanmar civil society's understanding of risks to users related to their digital footprints by providing sufficient funding for the complainants to commission an independent ICT eco-system study on the risks to end users in challenging operating contexts, including Myanmar. The study will be conducted with the primary objective to protect end users in Myanmar, but should also be relevant to other jurisdictions. It will be conducted by an internationally recognized and independent person or organisation, proposed by the mediators, with credible knowledge of the human rights risks of ICT. The study will also identify other relevant players in the ICT eco-system that have contributed to Myanmar ICT users' digital footprint and could contribute to the identification and mitigation of ICT risks to end-users."*

The study has been concluded and reported to the parties. The delivery includes a summary in English and Burmese to the benefit of the public.

3.4 How can companies in disengagement situations increase their leverage and mitigate risks in collaboration with others? (Question #8)

It should first be noted that leverage will be determined by the situation. A military coup forcing a company to disengage will render the company with little to no leverage compared with a voluntary and planned disengagement.

Engaging in multistakeholder initiatives and dialogue, as far as M&A conditions and regulations allow, is a good avenue to increase leverage. Telenor also recommends companies to uphold commitment to transparent external communication throughout a crisis, as far as possible.

Conducting pre-sale and at sale human rights due diligence, applying the UNGPs and OECD Guidelines, will also increase understanding of risks, opportunities and impacts and thus of leverage and the ability to prepare and mitigate.

3.5 What could responsible disengagement look like in the context of the present case? Question 9.

It is important to note that Telenor's exit from Myanmar was a forced exit. Telenor assessed all possible options, as described in the answers to questions 1-4 above.

Traffic data deletion was thoroughly assessed for all options. State of emergency and martial law had been declared in many geographical areas, including where Telenor's datacentre was located. Should Telenor have ordered employees to delete data they would have been in danger of death penalty and execution without trial. The historical traffic data was retained in digital format and on physical tapes. Purging of such data would have been time-consuming, and most likely discovered by the military regime before concluded, thus leaving employees at serious risk. It should be noted that the records included traffic data, such as information on usage of phones and which towers SIM cards connect to, but not any contents of the communication conducted by customers, such as phone conversations or content of messages sent by customers. Deleting the data was not an option in the sales scenario, both as the company relies on those systems for continued operations, and, most importantly, to ensure employee safety.

Continuing the operations was not an option, as that would have been in breach of Telenor's human rights commitments as well as of sanctions. A sale was the only viable solution. Telenor was able to protect our employees and ensure a continued fourth mobile operator in Myanmar.. Even if Telenor had been able to surrender the license or abandon the business the situation with regards to privacy would have been the same for the customers. They would then have had to rely on the remaining operators which faced the same requirements

See further in answers to questions # 1-4.

3.6 What can be appropriate remedy mechanisms and remediation for handling negative impacts related to telecommunications companies disengaging from conflict-affected areas? (Question #10)

Telenor had invested in, planned for, and would have wanted to continue operating in Myanmar, building infrastructure and providing millions of customers with means of communications. Telenor was forced to disengage, thus options for remediation were limited.

Telenor has pursued all of the several remedial actions defined in the public mediation MoU of this case before the NCP, except one remaining - to define a digital security relief mechanism.

Telenor acted on the action points defined in the MoU;

a) Continued engagement with stakeholders and rightsholders, which included Telenor providing Myanmar civil society representatives with specific information about the specific actual and potential risks associated with the digital eco-system and the sale of Telenor Myanmar. Telenor also initiated a Human Rights Expert Forum to share learnings and insights. A report summarising the discussions is available here:

https://www.telenor.com/binaries/sustainability/responsible-business/human-rights/telenor-human-rights-expert-forum/Telenor%20Human%20Rights%20Expert%20Forum%20Report.pdf

b) Conducting an independent ICT Eco-System Study, funded by Telenor, to enhance Myanmar civil society's understanding of risks to users from their digital footprints. Please see our response under question 7.

c) Exploring, as a follow-up action from the ICT eco-system study, how an independent Myanmar digital security relief mechanism could be established to provide support (financial, legal, training, etc.) to Myanmar citizens facing risks and impacts associated with their digital footprint. Please see our response under question 12.

d) Revisiting Telenor's assessment of risks to former employees, to determine whether there were any additional risks to be addressed. Please see our response under question 13.

e) Telenor conducting an internal assessment of lessons learned, including on how to have a responsible market entry and exit, from their work in Myanmar. This

assessment was informed by dialogue between Telenor and civil society organisations in the context of the OECD process.

f) Creating lesson-sharing opportunities, based on Telenor's disengagement process in Myanmar and especially with civil society and rightsholders in Myanmar as well as in other high-risk regions. Please see our response under question 6.

g) Following up on the implementation of the MoU with regular (monthly) check-ins, with the aim to reach a full agreement by the end of October 2022.

h) Publishing of the MoU and joint statement: The parties and the NCP published the text of the MoU and a joint statement on the state of the mediation process on the 28th of October 2022. The parties also agreed to maintain confidentiality on the mediation and any additional information discussed.

3.7 **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? (Question #11)**

In addition to Telenor actions for risk mitigation when exiting Myanmar as described in this document, see answers to Question 10. above.

3.8 **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? (Question #12)**

A digital security relief mechanism is a framework designed to provide support and protection to individuals and communities facing digital security threats. The aim would be to enhance the resilience of local governance structures and communities, particularly in regions experiencing political instability or conflict. It could include the provisioning of digital security tools and services. Advocacy for a digital security relief mechanism could focus on raising awareness, building capacity, and influencing policy to ensure the protection and support of individuals facing digital security threats. Actions could include raising digital security awareness, promoting access to digital security tools, and/or influencing policy and regulatory frameworks. Promoting digital security awareness comes with several challenges that can hinder its effectiveness. Addressing these challenges requires a concerted effort to raise awareness, provide education and training, allocate resources, and promote a culture of security within organizations and communities.

Telenor expressed its commitment to fulfil the MoU exploring how to establish and contribute to a 'digital security relief mechanism.' The objective of the mechanism

should be to build digital risk awareness in alignment with recommendations from the ICT Study. There is a need to address the practical difficulties of implementing the mechanism, as also stated in the study. Specifically, it needs to be addressed how to reach rightsholders without increasing risks to them, maintain people's confidentiality and security in the face of growing cyber threats, mitigate the risks of corruption, and recognise Telenor's lack of any operational capacity on the ground.

The ICT Study, which was commissioned in response to a general lack of data and knowledge as to digital risks, did not define such a mechanism, but listed eleven key questions for consideration in the exploration of a potential digital security relief mechanism. The Study indicates that any digital security relief mechanism should be centred on building digital risk awareness, providing support to Myanmar citizens, both inside and outside the country, who are today facing risks and impacts associated with their digital footprint. As the ICT Study says on this point: *"There are practical challenges in the Myanmar context to implementing a digital security relief mechanism, among them ensuring the right support reaches the right individuals and groups without increasing the risks they and others may face."*

Risks, practicalities and potential governance relating to such a mechanism must be considered, including human rights risks and impacts of both financing and supporting. There are, in other words, challenges in the Myanmar context to implementing a digital security relief mechanism, among them ensuring that the right support reaches the right individuals and groups. In practical terms, this includes how support could be delivered safely without introducing additional risks to recipients or others, and what connections would be needed on the ground to deliver support.

Further to the proposed considerations put forward in the study, the following aspects should be considered;

a) The fact that Telenor no longer has operations in Myanmar: Telenor does not have infrastructure, licenses, personnel, resources, and leverage in the country.

b) People safety risks: A solution directed towards beneficiaries within Myanmar must have as highest priority to safeguard the health and safety of people in any way involved in the administration as well as in the receiving end of a solution.

c) Confidentiality risks: A digital security relief mechanism will be subject to cyberthreats.

d) Corruption risks: Myanmar ranks number 162/180 in the 2023 Transparency International Corruption index: '2023 Corruption Perceptions Index'.

3.9 **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? (Question #13)**

In our experience, the way a company chooses to disengage from the country will be important, not least to remedy any current and future harm to employees. Furthermore, continuing to keep the safety of former employees a key priority after the exit is important. That is why Telenor is not conveying any information that could put former employees at risk, and this is a key element in avoiding harm to former employees.

Referring to our answers throughout this document, the sale option was least detrimental to employees and was the only option where their safety and livelihood could be ensured. In addition, Telenor did a risk assessment together with external expertise after the closure of the sale to secure if there were new and additional risks that had occurred to Telenor former employees. Telenor's internal Audit & Investigation (GIA&I) team offered access to the Hotline channel where former employees could raise their concerns, and GIA&I also offered to travel to a geography outside of Myanmar to meet former employees there for interviews.

3.10 **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? (Question #14)**

Telenor proposes the following key action points;

- The parties, as well as the NCP, should without further delay publish the ICT Study summary in English and Burmese.

- The outcome of the case should include sharing of the Myanmar learnings made available by Telenor, as well as the more general learnings from the Human Rights Expert Forum initiated by Telenor, available here:

https://www.telenor.com/sustainability/responsible-business/human-rights/telenor-human-rights-expert-forum/

While the forced exit and subsequent risks pose critical limitations, Telenor has continued to explore options in line with the MoU and with support from external subject matter experts. These will be assessed and aligned with ongoing Human Rights & Digital Inclusion efforts in the first half of 2025.

3.11 **What progress should be expected within one year? (Question #15)**

- Sharing Learnings: The parties should identify and set up a depository, external from the parties, on what Telenor has published about its Myanmar

entry and forced disengagement. Telenor should continue sharing its experiences and learnings with others (e.g., in the context of the GNI and GSMA).

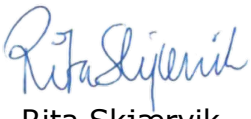
- Leverage: The parties should contribute to continued joint leverage as to rule of law and protection of human rights in the region, e.g. through active membership in the Global Network Initiative.

- Digital security relief mechanisms: As part of its sustainability strategy, Telenor has committed to support wider initiatives to build digital safety and security understanding among ICT users. Telenor continues to explore, based on the outcomes of the mediation, what options there are for Telenor to engage in.

* * *

Telenor trusts that the above responses address the NCP's inquiries. Should the NCP require further information or dialogue, we remain at your disposal.

Best regards



Rita Skjærvik

Execute Vice President People Sustainability & External Relation