National Contact Point
for Responsible Business
Conduct | Norway

Oslo 11 December 2025

Final Statement

Centre for Research on Multinational Corporations (SOMO) on behalf of 474 Myanmar-based civil society organisations vs. Telenor ASA

As stated in the Procedural Guidelines of the OECD Guidelines for Multinational Enterprises on Responsible Business Conduct, following conclusion of a Specific Instance and after consultation with the parties involved, the NCP will make the results of the procedures publicly available. As Specific Instances are not legal cases and NCPs are not judicial bodies, NCPs cannot directly order compensation nor compel parties to participate in a conciliation or mediation process.

This final statement describes the issues raised, the procedures initiated by the NCP to examine the issues and the conclusion of the NCP. It also includes recommendations to the enterprise on the implementation of the Guidelines.

Contents

1. Executive summary

1. On 27 July 2021, the Norwegian National Contact Point for Responsible Business Conduct (NCP) received a complaint from the Centre for Research on Multinational Corporations (SOMO) on behalf of 474 civil society organisations ('the Complainants') relating to the operations of Telenor Myanmar Ltd. The Complainants contended that Telenor failed to observe the recommendations of the OECD Guidelines for Multinational Enterprises on Responsible Business Conduct (the OECD Guidelines) with respect to risk-based due diligence, stakeholder engagement and disclosure in their disengagement from Myanmar.
2. The NCP accepted the complaint for further consideration in its Initial Assessment of 27 September 2021. Both parties accepted the NCPs offer of good offices. Formal mediation was deferred at the request of Telenor, based on serious concerns for the security of personnel. Mediation was held in June 2022, after which the Parties arrived at a memorandum of understanding (MoU) that captured the status of the mediation discussions, the agreements and acknowledgements reached, and a path forward for further mediation and agreement. The mediators convened several meetings with the parties individually and jointly and actions were taken to implement the MoU.
3. A final mediation session was planned for the spring of 2024 to discuss follow-up actions to the ICT ecosystem study, including a digital security relief mechanism. The session was cancelled, and the mediation came to an end without full agreement. The parties have differing views on the reasons for this. It seems that the main point of disagreement concerned the process to agree on, and the nature of, a digital security relief mechanism.
4. The Specific Instance was formally transferred back to the NCP on 11 September 2024, together with the closing statements from each party. The NCP proceeded to assess the outcomes achieved through the dialogue and commends the parties for the progress made through the MoU and efforts taken to implement the agreements. The NCP found that the remaining issues to be examined centre around two questions: 1) Did Telenor carry out due diligence in line with the Guidelines in relation to the exit from Myanmar? 2) Should Telenor play a role in remediation of adverse impacts, and if so, what role would be appropriate?
5. The NCP bases its examination on information submitted by both parties, the MoU, and information that is in the public domain. The NCP has found that Telenor did not carry out ongoing human rights due diligence commensurate to the severity and likelihood of all the adverse impacts with which the company was involved in in Myanmar. For example, it was not in accordance with the Guidelines to systematically prioritise one set of rightsholders, i.e. Telenor's own employees. The NCP has also found that Telenor's ability to mitigate risks for all those who were seriously at risk most likely was more limited than it could have been if the human rights due diligence and risk assessments as from the time of entry had identified and addressed the most serious risks and, as part of this, encompassed responsible exit scenarios.

6. The NCP is of the view that Telenor should take an active role in remediation to the extent of its contribution to adverse impacts by further follow-up of the commitments in the MoU. The NCP recommends Telenor to continue its engagement and commitment to explore, concretise, design and implement, including to provide financial support to, a Myanmar digital security relief mechanism, which is described in the ICT Ecosystem Study as a type of fund, in cooperation with other actors linked to ICT-related impacts in Myanmar and the region.
7. At a late stage in the NCP's handling of the case, legal proceedings were initiated against Telenor in the Oslo City Court. The plaintiffs claim compensation and allege that Telenor shared user data with the junta after the coup and that arbitrary detention, torture and that in one case, execution followed as a consequence. Telenor requested the NCP to defer its proceedings to await the outcome of the legal proceedings. After considering the request, the NCP decided to conclude the Specific Instance and issue a Final Statement.

2. Background and procedures

2.1. The NCP and its role

8. The OECD Guidelines are recommendations jointly addressed by governments to multinational enterprises operating in or from adhering countries. They provide non-binding principles and standards for responsible business conduct in a global context consistent with applicable laws and internationally recognized standards. The recommendation from governments that enterprises observe the Guidelines is distinct from matters of legal liability and enforcement. The Guidelines are supported by National Contact Points (NCPs), established by adhering governments to promote and implement the Guidelines.
9. According to the Guidelines, the NCP will contribute to the resolution of issues that arise relating to implementation of the Guidelines in specific instances. Where the issues raised merit further examination, the NCP will offer good offices to help the parties involved to resolve the issues. The Norwegian NCP handles specific instances in accordance with the procedures in the OECD Guidelines and the NCP's case-handling procedures.[1]
10. As the NCP received this Specific Instance in 2021, the basis for handling and examining the case is the 2011-version of the OECD Guidelines and related procedures. The recommendations from the NCP are, however, forward-looking, and therefore also the updated Guidelines from 2023 form the foundation for the recommendations from the NCP.

[1] Case-handling procedures

2.2. The parties

11. Telenor ASA is a majority state-owned multinational telecommunications company headquartered in Oslo, Norway. Telenor Myanmar was a wholly owned subsidiary of Telenor ASA, and until Telenor left Myanmar, headquartered in Yangon, Myanmar.

12. SOMO is an independent, not-for-profit organisation registered in Amsterdam, The Netherlands, focusing on the impact of the activities of multinational enterprises on people and the environment. SOMO monitors the implementation of the OECD Guidelines and advocates for strong corporate accountability frameworks to address global governance gaps. SOMO filed the complaint on behalf of 474 Myanmar-based civil society organisations (CSOs). The local CSOs are anonymous due to the human rights situation in Myanmar. The identities of the CSOs have, however, been disclosed to the NCP, and the NCP has reviewed the list of organisations on a confidential basis.

2.3. Submissions from the Parties

13. The NCP received the submission from SOMO on behalf of 474 Myanmar-based CSOs on 27 July 2021. The complaint alleged non-adherence to the OECD Guidelines by Telenor ASA in relation to its disengagement from its Myanmar operations.

14. The Complainants contended that Telenor's sale of its Myanmar business to M1 Group,[2] a Lebanese investment company, failed to meet the standards of responsible disengagement set out in the OECD Guidelines in three key respects.[3] First, that Telenor failed to conduct appropriate risk-based due diligence and has failed to seek to prevent or mitigate adverse human rights impacts to its customers potentially arising from the sale of its Myanmar operations. Second, that Telenor failed to meaningfully engage with relevant stakeholders in relation to the sale of Telenor Myanmar to M1 Group. Third, that Telenor has not acted in accordance with OECD standards on disclosure and communication about due diligence in relation to its decision to disengage from its Myanmar operations.

15. The complaint alleged that Telenor Myanmar failed to uphold several provisions in Chapter II (General Policies), Chapter III (Disclosure) and Chapter IV (Human Rights) of the OECD Guidelines. The submission also referenced recommendations for responsible disengagement in the OECD Due Diligence Guidance for Responsible Business Conduct (2018).

16. Telenor responded to the submission from SOMO on 12 August 2021, expressing serious concerns with respect to the challenging situation in Myanmar following the military coup. According to Telenor, the decision to disengage was extremely challenging and was taken as a last resort. Telenor carried out "thorough assessments on the available alternatives prior

[2] The Complainants stated that two lawsuits have been commenced against MTN Group Limited (MTN). M1 limited, a subsidiary of M1 Group Limited, held 6.44 percent of shares in MTN. See pages 6 – 7 of the complaint.
[3] The Complainants also contended that the enterprise has failed to act in accordance with the United Nations Guiding Principles on Business and Human Rights (UNGPs). The NCP considers submissions relating to alleged non-observance of the OECD Guidelines, and the OECD Guidelines were updated and aligned with the UNGPs in 2011.

to the decision to sell."[4] The company stated that the ability to continue adhering to responsible business conduct, international law and human rights principles were key factors in these assessments. The security and safety of Telenor personnel and their continued employment were important factors.[5]

17. In their response, Telenor described their efforts with respect to the issues raised in the submission regarding transparency on the situation, their efforts regarding stakeholder engagement and assessments of how to proceed. Telenor held that they were in a position where it would no longer be possible to continue operations in line with its policies and internal and external requirements following the military takeover, and that the company was forced to sell as a last resort. Telenor considered that the sale of Telenor Myanmar would secure access to service for 18 million subscribers, hospitals and banks, as well as maintaining a fourth operator independent of the military regime that could secure continued employment for the employees of Telenor Myanmar.

2.4. Initial assessment

18. In its initial assessment of 27 September 2021, the Norwegian NCP decided to accept the submission for further consideration.[6] The decision was taken following an elaboration of the six criteria outlined in the commentary to the Procedural Guidance in the OECD Guidelines (2011) and the Procedural Guidelines of the Norwegian NCP (2014).

2.5. Proceedings of the NCP after the initial assessment – good offices

2.5.1 Dialogue and mediation

19. Both parties accepted the NCPs offer of good offices. With the approval of the parties, the NCP appointed Mark Stephens and Anna Triponel as external mediators – a mediation team with expertise on business and human rights in the telecommunications sector, mediation and Myanmar-experience. The NCP encouraged the parties to engage in the dialogue as soon as possible. Formal mediation was, however, deferred at the request of Telenor, who invoked serious concerns about the security of personnel. Mediation was delayed until the company could complete its exit from Myanmar in a way that the company considered safe. The mediators held pre-mediation meetings with the parties individually and together and prepared a framework for mediation.

20. An in-person mediation took place between the 13 and 15 June 2022 in Stockholm, Sweden. The mediation entailed the initiation of a meaningful and respectful exchange of information and views on Telenor's human rights due diligence when it entered Myanmar, while operating in Myanmar – both before and after the coup – and around its decision to sell

[4] Telenor's response to the complaint, 12 August 2021, page 1.
[5] Telenor's response to the complaint, 12 August 2021, page 1.
[6] Initial Assessment of 27 September 2021: SOMO on behalf of 474 Myanmar-based civil society organisations vs. Telenor ASA.

Telenor Myanmar. It also discussed the wider digital ecosystem of which Telenor is a part, including services on the internet, and in which users operate.

21. After the initial mediation in June 2022 in Sweden, the Parties arrived at a preliminary memorandum of understanding (MoU) that captured the status of the mediation discussions, the agreements and acknowledgements reached thus far, and a path forward for further mediation and agreement. The parties agreed to publish the MoU.[7]

2.5.2 Memorandum of Understanding

22. In the MoU, the parties acknowledged and agreed on the following key points:

    a. The responsibility to conduct human rights due diligence applies to a sale process, including Telenor's decision to sell Telenor Myanmar.

    b. There were severe human rights risks associated with each of the options to sell Telenor Myanmar following the military coup and that all the options considered by Telenor entailed severe risks to customers and to the 734 Myanmar-based employees, as well as risks to local contractors, suppliers and society-at-large.

    c. As a result of the coup, there are currently serious risks to end users in Myanmar connected to how their information and communications technology (ICT) data can be misused against them by the military junta; risks that have increased following the coup. The parties acknowledged that there are risks to some former Telenor Myanmar employees, such as social and physical punishment for association with the military.

    d. End-users are facing both a holistic risk, due to the junta's possible use of users' digital footprints to target them, their families and their contacts, as well as specific risks connected to traffic and customer registration data held by Telenor Myanmar.

    e. Telenor Myanmar was one of the many players of the digital eco-system in Myanmar and the metadata and content data generated by users through internet services external to Telenor also makes up the users' digital footprint.

    f. The risks involved in a sale to an international buyer differ from the risks involved in a sale to a buyer associated with the junta. The parties agreed that the human rights risks from the sale of Telenor Myanmar became more salient when it was made clear that the regulatory approval was contingent on local ownership.

23. The parties held different views on risk prioritization, disclosure and what kind of stakeholder engagement would have been possible and expected by the OECD Guidelines as part of the human rights due diligence related to the sale of Telenor Myanmar. They recognized, however, the need for further clarity on how meaningful stakeholder engagement with customers can be conducted during a sale process in a challenging operating context.

24. The parties also agreed on several follow-up actions in the MoU:

[7] See Memorandum of Understanding (MoU).

a. Continued **engagement with stakeholders and rightsholders**, which includes 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.

b. Conducting an independent **ICT Ecosystem Study**, funded by Telenor, to enhance Myanmar civil society's understanding of risks to users from their digital footprints. The study would also identify other relevant players in the ICT eco-system that have contributed to Myanmar ICT users' digital footprint and could contribute to identifying and mitigating ICT risks to end-users.

c. Exploring, as a follow-up action from the ICT ecosystem 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.

d. **Revisiting Telenor's previous risk assessment process**, to determine whether there were any additional risks to be addressed.

e. **Internal assessment of lessons learned by Telenor**, including on how to ensure a responsible market entry and exit from their operations in Myanmar. This would be informed by dialogue between Telenor and civil society organisations in the context of the OECD process.

f. **Creation of 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.

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

25. Following the MoU, the mediators convened a number of meetings with the parties individually and jointly and actions were taken to implement agreements in the MoU.

2.6. Follow-up of the MoU

26. The parties have informed the NCP of their positions upon the conclusion of the mediation and shared a summary of the ICT ecosystem study (see Attachment 2). The following is a summary of information received from the parties upon the conclusion of the mediation and addresses follow-up of the agreements made in the MoU.

2.6.1 Engagement with stakeholders and rightsholders

27. The parties agreed that Telenor would provide Myanmar civil society representatives with specific information regarding actual and potential risks to digital rights and freedoms in Myanmar under the military junta, associated with the digital ecosystem and the sale of Telenor Myanmar.

28. The complainants state that Telenor frequently provided information to the complainants only after it was published on the corporate website. For this reason, they state that the engagement was discontinued almost immediately after it was started.[8]

29. Telenor states that they in November 2022 hosted a closed discussion on digital ecosystem risks between the complainants and its internal experts in cybersecurity and the digital ecosystem risks in Myanmar. The session aimed to address and clarify the complainants' questions about the risks to users in Myanmar's ICT ecosystem and the sale and transfer of user data.[9]

2.6.2 Engagement with former Telenor Myanmar employees

30. The parties agreed that Telenor would revisit its previous risk assessment process to determine whether there were additional risks to be addressed.

31. The complainants state that Telenor Myanmar employees faced severely increased risks of harassment and violence due to their association with Telenor following the exit of Telenor, particularly due to the way in which Telenor exited. They are of the view that Telenor did not provide secure enough channels for employees to feel comfortable discussing their security concerns. Given the severe risks they faced, it was not acceptable to the former employees to be interviewed by anyone from Telenor's internal audit office because the auditor was still a Telenor employee that reported directly to the board of Telenor, and the former employees did not feel that their identity could be protected.[10]

32. Telenor states that their main communication channel with former employees was the Internal Audit and Investigation (GIA&I) hotline, which Telenor committed to continue monitoring. Telenor shared information with the complainants about how to access the mechanism. After further reports from the complainants of former employees' fears of reprisals for using the hotline, Telenor offered additional communication channels and safeguards. Telenor and GIA &I agreed to increase safety and confidentiality by allowing former employees to use pseudonyms and proposed to meet the employees in person in a safe place in Thailand, as well as using an end-to-end encrypted channel to virtually meet the individuals at risk. After the closure of the sale, Telenor did a new risk assessment with Control Risks, a global risk consultancy, to assess if there were new and additional risks that had occurred to former employees. No such risks were identified by them. Telenor states that the complainants did not accept offers to meet for interviews in Bangkok.[11]

33. The complainants state that the former employees still did not feel safe enough to discuss current security concerns and human rights impacts through the hotline and offered channels. They offered to provide anonymized written feedback about their situation to Telenor until Telenor could provide a secure way for them to engage but Telenor insisted

[8] Complainants' observations following failed mediation of 9 September 2024, page 3.
[9] Telenor Statement of Transfer of Complaint to the Norwegian NCP of 29 August 2024, page 5.
[10] Complainants' observations following failed mediation of 9 September 2024, page 3.
[11] Telenor Statement of Transfer of Complaint to the Norwegian NCP of 29 August 2024, pages 5 – 6 and page 13.

that the employees would need to participate in an interview (either physically or online) which according to the complainants would expose their identity to the auditor.[12]

2.6.3 Independent ICT Ecosystem study

34. The parties worked over several months to select experts to conduct the study and to agree on the terms of reference for the study.

35. The work commenced in June 2023, and the study was delivered in April 2024.[13] The ICT study identified various digital actors in Myanmar, the types of personal data collected by them, surveillance methods used by the Junta, and potential actions for risk mitigation and remedy. It also provided recommendations for telecommunications companies in general, Telenor, civil society, academia and research organizations on how to prevent and mitigate risks, constituting best practice in Myanmar and elsewhere.

2.6.4 Digital security relief mechanism

36. As a follow-up action from the ICT Ecosystem Study, the parties agreed in the MoU to explore how an independent Myanmar digital security relief mechanism could be established to provide support to Myanmar citizens facing risks and adverse impacts associated with their digital footprint. The study did not define what would constitute a digital relief mechanism but listed eleven key questions for consideration in the exploration of such a mechanism. A 'digital security relief mechanism' is described as a fund of some kind, focused on reducing risks relating to digital footprints. The study noted the following:

> "Interviewees for the study had a variety of views on what such a mechanism could offer. Although human rights defenders (HRDs) are increasingly aware of the risks relating to digital footprints and the steps they can take to help to reduce risks to their safety and security, many lack the resources to be able to use all technical safeguards available. There is also a considerable need for greater digital security awareness for the wider population. Interviewees also raised the need for resources to support the work of Burmese HRDs, journalists and academics both inside and outside the country.
>
> There are practical 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 without increasing the risks they and others may face."[14]

37. Further to this, the study recommends the Parties to the Specific Instance to consider the risks, practicalities and potential governance relating to such a mechanism. It recommends exploring what role the Parties, together or independently, could take in relation to remedy more broadly, in particular when it comes to the development of guidance for responsible exit / disengagement informed by this case and greater multistakeholder collaboration to consider remedy generally within the ICT sector.[15]

[12] Complainants' observations following failed mediation of 9 September 2024, pages 3 – 4.
[13] A summary of the study is appended to the Final Statement.
[14] Myanmar ICT Ecosystem Study – a summary, February 2024, page7.
[15] Myanmar ICT Ecosystem Study – a summary, February 2024, page 9.

38. Telenor has expressed its commitment to fulfilling the MoU and exploring how to establish and contribute to the digital security relief mechanism.[16]

39. Prior to the final round of mediation, the complainants proposed a concrete concept for the mechanism – a Myanmar Digital Resilience Mechanism. They also shared this proposal with the NCP and Telenor. Such a mechanism, they suggest, would support digital risk awareness and the development of decentralized digital infrastructure as well as support the digital security of Myanmar citizens, including by funding existing or developing safe alternative forms of communication, providing VPN access, and emergency grants. They proposed that the mechanism be managed and overseen by a consortium of international and local organizations. They state that Telenor's financial contribution to the fund should amount to USD 180 million, equivalent to USD 10 per former Telenor Myanmar customer, which is similar to the initial cost paid by the 18 million Myanmar customers who purchased Telenor SIM cards and credit packages.[17]

40. In their submission, Telenor states that the complainants' proposal introduced new requirements that in their view deviate from the process defined in the MoU and informed by the ICT study. Telenor does not believe that due process as recommended in the ICT study was followed in reaching a practical solution to what such a mechanism for Myanmar could be. They also state that the parties disagree on the objective of such a mechanism. Where the complainants focus on digital infrastructure and emergency grants as well as digital risk awareness, Telenor is of the view that the only objective of the mechanism should be to build digital risk awareness in the country.[18]

2.6.5 Assessment and sharing of lessons learned

41. In 2022 and 2023, Telenor conducted an internal review of its disengagement risk assessment process, led by a third-party auditor (the Norwegian law firm Wikborg Rein). The review included workshops with all employees involved in the Myanmar exit as well as four external civil society organizations. The conclusions were shared with the mediators and complainants in a closed session and publicly on the Telenor website. During the review process, Telenor invited the complainants to provide information on Telenor's actions before and following the coup, as well as before and after the sale. Telenor states that the complainants did not respond to the invitation to engage with the internal assessment process.[19] Telenor states that they have continuously published information on the Myanmar exit and lessons learned, taken part in international events and closed roundtables to share experiences of working in conflict-affected markets.[20]

42. The complainants state that they were invited to give input to Telenor's internal review mentioned above and the sharing of lessons learned. They had requested clarification on the outcome of the internal review, voicing that they did not feel comfortable without

[16] See MoU and submission from Telenor to the NCP of 20 January 2025, page 17.
[17] Complainants' proposal for the focus of the mediation on 2-3 May 2024.
[18] Telenor Statement of Transfer of Complaint to the Norwegian NCP of 29 August 2024, page 16.
[19] Telenor Statement of Transfer of Complaint to the Norwegian NCP of 29 August 2024, page 14.
[20] Telenor Statement of Transfer of Complaint to the Norwegian NCP of 29 August 2024, pages 14 – 15.

knowing how their perspectives were contributing to the review.[21] According to the complainants, Telenor never provided the complainants with such clarification. The complainants furthermore state that Telenor conducted an internal learning process that included input and reflections from business and human rights experts on its disengagement process. According to the complainants, Telenor never informed them about this process, and they only heard about it following the public release of its report.[22]

2.6.6 Regular check-ins

43. The parties stayed in constant communication in the months following the in-person mediation and the mediators facilitated bi-weekly calls to discuss the ICT study and other MoU action points.

2.7. Closure of the mediation, issues for further examination and the NCP's post-mediation procedure

44. A final mediation session was planned for the spring of 2024. The purpose was to discuss follow-up actions to the ICT ecosystem study, including setting up a digital security relief mechanism. Unfortunately, the session was cancelled shortly before it was planned to take place. The parties have differing views on why the final round of mediation did not take place. It seems that the main point of disagreement concerns the process to agree on, and the nature of, a digital security relief mechanism.
45. The parties did not reach a final agreement. At the closure of the mediation, the parties were asked to submit closing statements to the mediators. The Specific Instance was formally transferred back to the NCP on 11 September 2024, together with the closing statements from each party.
46. The NCP assessed the outcomes achieved through the dialogue and found that the remaining issues to be examined centred around the following questions:
    a. Did Telenor carry out risk-based due diligence, including stakeholder engagement and communication, in line with the Guidelines in relation to the disengagement from Myanmar?
    b. Should Telenor play a role in remediation of adverse impacts, and if so, what role would be appropriate?
47. The NCP sent the parties a list of questions on 31 October 2024 (Attachment 1), to provide a basis for the NCP's assessment of these issues. The NCP received the response from Telenor on 20 January 2025. The NCP received the response from the complainants on 31 January 2025. Following this, the NCP continued its examination of the case and the preparation of the Final Statement.

[21] Complainants' observations following failed mediation of 9 September 2024, page 4.
[22] See complainants' observations following failed mediation of 9 September 2024, page 4. The report is available online and has been shared with the NCP: Telenor Human Rights Expert Forum Report March 2024.

48. The complainants submitted new information to the NCP on 1 August 2025, with reference to an article in the Norwegian newspaper Dagens Næringsliv (DN). The NCP shared this with Telenor for comments. Subsequently, from 20 August onwards, the Norwegian Broadcasting Corporation (NRK) published extensive articles on Telenor's exit from Myanmar. The articles were based on investigation and sources providing new and detailed information about Telenor's handling of the military junta's requests for historical customer data and other matters.[23] Upon the NCP's request, Telenor commented on the information given in the NRK-articles. Telenor's replies were shared with the complainants for any comments, and the NCP received the reply from SOMO on 28 August 2025. Subsequently, Telenor alleged that SOMO had breached its duty of confidentiality in its statements to the media about the mediation. SOMO denied this in their reply to the NCP on 10 September 2025.

49. A draft Final Statement was sent to the parties for comments on 5 November 2025. Both SOMO and Telenor submitted comments by the deadline set by the NCP of 19 November 2025. The NCP has considered the comments in completing the Final Statement, in line with the NCP case-handling procedures. The NCP has also taken note that two criminal complaints were filed against Telenor relating to allegations of breaches of sanction rules in relation to the Myanmar operations. One was filed by the Ministry of Foreign Affairs and the other by ICJ Norway and Justice for Myanmar. The Norwegian Policy Security Service (PST) concluded that there was no reasonable basis for investigation. The National Prosecuting Authority has since sent the case back to PST for further investigation.

2.8. Parallel proceedings

50. On 6 October 2025, SOMO informed the NCP that civil litigation will be filed against Telenor on behalf of individual customers of Telenor Myanmar. The NCP requested the parties to submit any comments regarding the parallel proceedings in relation to the NCP process. The complainants were of the view that the announced potential civil litigation should not affect the NCP process in any way. Telenor asked the NCP to defer further consideration of the case until the announced legal proceedings have been concluded.

51. The notice of claims[24] against Telenor is dated 6 October 2025 and indicates that the claimants are several Myanmar citizens, including families of deceased, and non-profit organisations. The plaintiffs will claim compensation based on Telenor's responsibility as an employer for actions or omissions by its employees.[25] The basis for the claim seems to be that Telenor shared user data with the junta after the coup and that arbitrary detention, torture and that in at least one case, execution followed as a consequence.

52. The NCP has decided to conclude the Specific Instance and issue a Final Statement. According to the Guidelines, the NCP is not precluded from offering its good offices to the parties if parallel proceedings have been conducted, are underway or are available to the

[23] Historical customer data includes all data from customers until Telenor disengaged from Myanmar. It must be noted that such data only includes meta-data and not content data.
[24] In Norwegian: "Prosessvarsel".
[25] In Norwegian: "arbeidsgiveransvar", based on the damages act ("skadeserstatningsloven") § 2-1.

parties.[26] The same must apply at the final stages of the Specific Instance procedure. In the view of the NCP, going forward with the Final Statement does not create any serious prejudice for either of the parties or any unjust interference with the upcoming court proceedings. The NCP points out that the Final Statement addresses expectations under the Guidelines, and not legal requirements. The legal responsibilities for Telenor must be assessed and decided by the courts of law and may, of course, differ from the findings of the NCP, which are based on the Guidelines alone. Furthermore, the Specific Instance is in its very last stages and the situation, in fact, does not differ from a situation where the Final Statement is issued in time before legal proceedings are commenced, and the mere availability of legal proceedings should normally not defer further proceedings at the final stage of a specific instance procedure.

53. The NCP underscores that, although there might be some overlapping issues, the Final Statement does not deal with individual cases nor impacts on specific individuals. Further, there are limitations as regards the NCP's factual basis for its examination, see section 3.2 below.

54. Finally, the NCP adds that the most important outcome of this Specific Instance – the recommendations to the parties – are forward looking, whereas the legal proceedings deal with claims for compensation for loss suffered. It is of great importance that the commitments undertaken in the MoU, especially Telenor's engagement and commitment to explore, concretise and implement a Myanmar digital security relief mechanism[27] continue without further delay. Thus, the NCP considers that going forward and concluding the procedure with a Final Statement could make a positive contribution to the resolution of the issues raised in the Specific Instance.

3. Examination by the NCP

3.1. The NCP's finding of facts – the context

3.1.1 Introduction

55. At the outset, the NCP takes note of the fact that, at the time of Telenor's entry to Myanmar, there was a high degree of optimism relating to investments in the country after the dissolution of the military junta in 2011. The Norwegian government shared this optimism and encouraged Norwegian investments in the country. The Government's state ownership policy spells out the Government's expectations on responsible business conduct and due diligence. To what extent this was adequately followed up by the Government throughout the period in which Telenor had operations in Myanmar lies outside the scope of issues covered by this Specific Instance.

56. Telenor's contribution to the expansion of the telecommunications network and the services provided in Myanmar enabled connectivity and positive benefits for an estimated 18 million

[26] See the OECD Guidelines (2023), Part II, paragraph 35.

[27] See the recommendation in Chapter 5, paragraph 150 below.

users, facilitating access to healthcare and other public services, among other things. Telenor initially ran a very successful and profitable business in Myanmar. However, following the military coup on 1 February 2021, Telenor decided that it was not possible to continue its business in the country and sold its Myanmar operations to the Lebanese investment company M1 Group for USD 105 million. The sale, announced on 8 July 2021, was approved by the Myanmar authorities and completed on 25 March 2022. The final authorization by the Myanmar authorities was given under the condition that it was established a joint ownership between M1 Group and a local partner which also was the majority owner.

57. The NCP has previously reviewed Telenor's due diligence in relation to the entry to Myanmar in the Specific Instance *Committee Seeking Justice for Alethankyaw vs Telenor.*[28] In its Final Statement, the NCP noted that there were several positive features in Telenor's efforts to identify, prevent and mitigate human rights risks and communicate about these in Myanmar through public briefings and reporting. Human rights policies were included in contracts with vendors and business partners and followed up. Telenor engaged with stakeholders in Myanmar and internationally. Lawful intercept of real time communication was identified as a serious human rights risk as from the beginning of Telenor's engagement in Myanmar, especially since adequate legal safeguards were not established. Telenor advocated for a legal and regulatory framework for lawful intercept in line with international best practices and practiced a high degree of transparency around operations and risk assessments prior to and during the Myanmar operations. Nevertheless, the NCP noted in its Final Statement that Telenor's risk assessments and human rights due diligence failed to address the risks faced by the most marginalized groups, i.e. the Rohingya population.

58. The Specific Instance now before the NCP centres on Telenor's disengagement from Myanmar after the military coup in February 2021. This Specific Instance thus raises issues pertaining to Telenor's operations in Myanmar that were not covered by the abovementioned Specific Instance. The following factual context is relevant to this Final Statement.

3.1.2 The situation in Myanmar after the military coup

59. After the military coup in February 2021, the people of Myanmar, and particularly the political opposition and human rights activists, faced increased and severe human rights risks, including increased risks related to the potential misuse of ICT data by the junta. The UN Office of the High Commissioner for Human Rights has stated that in Myanmar shortly after the coup, the military "unilaterally amended and instrumentalised the legal framework to stifle free expression, justify arbitrary deprivation of liberty, and deny thousands of activists, journalists, and human rights defenders due process and fair trial rights."[29]

60. As established in the Myanmar ICT Ecosystem Study, impacts on the human rights of individuals from digital surveillance can be extremely severe in the context of conflict-

[28] See the Final Statement here.
[29] United Nations High Commissioner for Human Rights (2023). Situation of human Rights in Myanmar – Report of the United Nations High Commissioner for Human Rights, page 2.

affected and high-risk areas (CAHRAs), like Myanmar both before and after the coup, and include:

- surveillance leading to violation of the right to privacy – whether of communications, relationships, opinions, or home;
- surveillance having a chilling effect on freedom of expression and freedom of association and movement, leading to self-censorship of expression, opinion, religious practice and participation in protests;
- surveillance leading to arbitrary arrests and detention, torture, inhumane and degrading treatment, and extrajudicial killings;
- surveillance used to reinforce discrimination including facilitating forced labour of ethnic minorities.[30]

61. According to Telenor, the period that followed was extremely challenging for the company, its employees, customers and the Myanmar society as a whole:

> "[t]he challenges faced as a private company and a telecommunications operator were unprecedented, with dilemmas related to the safety and security of our employees, human rights concerns across the Myanmar society, and a legal and regulatory environment that no international guidelines or best practices have fully captured".[31]

62. Following the military coup, Telenor established a crisis management organisation, including all levels of the organization, headed by a Steering Committee. The Telenor ASA Board of Directors were involved on a regular basis. According to Telenor, due diligence and possible impacts were considered regularly on identified risk scenarios, including people security and human rights. In its submissions to the NCP, the company explains, without going into detail, that the risk picture was updated throughout the period from the coup to the exit. An exit plan for possible scenarios, which also covered human rights impacts, was developed. Telenor explains, in a general manner, that its human rights assessments "also included taking steps to mitigate potential adverse human rights impacts, while not risking lives of employees".

63. In general, it was important for Telenor to maintain connectivity for its customers and thereby give them continued access to different services, like health services. According to Telenor, the company set out clear principles for managing the crisis that followed the military takeover. A key principle was that no employee should have to risk their life or health – employee safety was always put first. Telenor states that another principle was that customer safety had to be ensured. At the same time, Telenor has stated that it "became impossible to be a telecom operator in Myanmar and uphold international standards and safeguard customers' rights under such circumstances".[32]

64. In its submissions to the NCP, Telenor explains that, after the military coup, they faced increasing security risks and threats to employees on the ground, and augmented government requests to activate lawful intercept equipment in the Myanmar operations.

---

[30] Myanmar ICT Ecosystem Study – a summary, February 2024, page 3.
[31] Outcomes of Telenor's internal learning process from the Myanmar engagement, Preamble from Telenor.
[32] L.c.

Activating lawful intercept of communication, which the military junta requested, would have been subject to Norwegian and EU sanctions and would have led to severe human rights risks to its users in the country.[33] In these circumstances, Telenor considered it impossible to remain in Myanmar and comply with its obligations regarding human rights and international best practices while keeping employees safe.[34]

65. Telenor is of the view that they were forced to exit Myanmar, especially by the order from the military Junta to activate lawful intercept. Faced with the situation after the coup, they analysed three options on how to exit: (1) surrender the license back to the government; (2) abrupt shut-down by immediate switch of the mobile network; or (3) sale of the business. Telenor concluded that selling the business was the least detrimental option, and the company subsequently entered into an agreement to sell 100 percent of the shares in Telenor Myanmar to the Lebanese investment company M1 Group.[35] From November 2021 it was known to Telenor that it was likely that a requirement for M1's acquisition of Telenor Myanmar would be that a majority of the shares should be resold to a local company with close ties to the military junta, Shwe Byain Phyu Group.

66. The MoU between the Parties in this Specific Instance establishes that there were severe human rights risks associated with each of the options explored by Telenor Myanmar following the military coup. It also acknowledges that all the options considered by Telenor entailed severe risks to customers and to the 734 Myanmar-based employees, as well as risks to local contractors, suppliers and society-at-large, see paragraph 22 above.

3.1.3 Was Telenor prepared for the change in operational context after the military coup?

67. Even though democratic reforms were introduced from 2011 and the election in 2015 has been labelled as the first free and democratic general election in Myanmar, the transition from military rule to civil democracy was never complete. While political liberalisation took place, the military was still in control. The Rohingya crisis in 2017 and the following ethnic cleansing and grave persecution of the population in parts of the country revealed the continued capacity and willingness of the military to use extremely brutal methods of oppression.

68. As indicated in paragraph 57 above, the NCP finds that Telenor's efforts to respect human rights prior to the coup in February 2021 seemed in many ways to be commendable. Several third-party human rights assessments were commissioned in addition to Telenor's own human rights risk assessments and due diligence processes. In 2020 Telenor commissioned an assessment of human rights risks in Myanmar by the consultancy Article One. This report was delivered to Telenor in January 2021, but the coup in February overtook Telenor's work with the findings in this report and its recommendations were not implemented. In the

[33] Software updates were required to make the interception software operational and were excluded through sanctions for supply and operation.
[34] Telenor Statement of Transfer of Complaint to the Norwegian NCP, 29 August 2024, page 1. See also Telenor Group, Continued presence in Myanmar not possible for Telenor (2021).
[35] Telenor Statement of Transfer of Complaint to the Norwegian NCP of 29 August 2024, page 2.

report, Article One makes the following observation about the latest developments in Myanmar:

> "Importantly, the demands from Myanmar authorities have become more severe and expanded in scope and frequency in the last year—adding significant human rights challenges to Telenor's operations. These demands have included requests for:
>
> 1. Network shutdowns and restrictions of internet services in Rakhine and Chin states;
>
> 2. Website blocking of independent media organisations;
>
> 3. Implementation of SIM registration;
>
> 4. Historical data on specific users, mainly related to serious crimes; and
>
> 5. Integration of technology to support real-time lawful interception of communications."

69. Against this backdrop, it is interesting that, according to Telenor's own set of learnings, "[t]he coup revealed that Telenor's existing (pre-coup) crisis management were not fully fit for purpose (i.e. were not especially useful in the context of the coup)".[36] Moreover, in its submission to the NCP, Telenor explains that it was "evident that risk assessments conducted before the coup had limited relevance" in establishing the company's first "risk picture" after the coup. Indeed, according to Telenor's submissions to the NCP, mitigating activities and exit strategies were only discussed and formed in February 2021, i.e. post-coup.

70. The NCP must conclude, based on the information available to it, that Telenor was not prepared for a situation like the one created by the military coup in February 2021. The risk-assessments and human rights due diligence processes had not encompassed the possibility of full military rule in Myanmar, and the company had no exit strategy in place before the coup. This is confirmed by a set of learnings from Telenor's process of engagement and disengagement from Myanmar, published in 2023 and referenced in a submission to the NCP. One of the key lessons learned concerns the issue of crisis preparedness:

> "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."[37]

[36] Outcomes of Telenor's internal learning process from the Myanmar engagement - Telenor Group.
[37] Ibid.

3.1.4 Authorities' requests for information

71. Requests for information by the authorities to achieve its aims were well known to Telenor from the start of its operations in Myanmar. Requests for e.g. historical user data may be legitimate, also in democratic societies, and are often used in connection with the investigation of serious crimes. However, such requests may also be misused by the authorities. Interception of communications and sharing of user data can potentially have serious impacts on the human rights of – in our case – Telenor's customers, including adverse impacts on the right to privacy and the right to security of persons, see paragraph 60 above. As agreed in the MoU, the human rights risks became more salient when it was made clear that the regulatory approval was contingent on local, majority ownership.

72. Demands from the Myanmar authorities had for many years before the coup included requests for integration and activation of technology to support real-time lawful intercept of communication[38] as well as requests for historical data on specific users and other requests. According to Telenor, the equipment for lawful intercept was never activated, but this was also a "red line" for Telenor, both because of its human rights implications and the EU sanctions pertaining to such equipment in Myanmar. Telenor did, however, install, test, and make the intercept technology "ready for use". A major concern for Telenor was the EU sanction on lawful intercept equipment that came into force in April 2018 and was implemented in the Norwegian Regulation of Export Control in July 2018.

73. As for requests for historical user data both before and after the coup, Telenor processed all requests from the authorities based on a set of rules outlined in its Authority Requests Manual. In the event that authority requests were determined to be unusual or pose substantial risks for adverse impacts on human rights, the request was, according to the Authority Requests Manual, to be escalated to the relevant function within a hierarchy of escalation points of contact, including the CEO and a task force consisting of cross-functional experts.

74. According to Telenor, 86% of such requests were complied with in 2019, 94% in 2020 and 96% in 2021. However, this changed after the coup, as Telenor, in fact, complied with all requests for historical customer data from the military junta. The table below includes the number of historical customer data requests for 2014-2021 and the percentage of requests met in 2019-2021, as published in Telenor's Authority Request Disclosure Report.

[38] See e.g. Phuy Phuy Kyaw, Open Technology Fund (2020): The Rise of Online Censorship and Surveillance in Myanmar, which provides information that the Myanmar MoTC called for a meeting on 31 January 2019 to discuss technical aspects of the lawful intercept systems, and the monitoring of voice and traffic data in the country was discussed. Telenor participated in the meeting. The Myanmar ICT Ecosystem Study refers to the report, see endnote 18 in the summary of the Study.

Year	Historical Customer Data Requests*	Requests Met
2014	9	No data available
2015	35	No data available
2016	51	No data available
2017	49	No data available
2018	64	No data available
2019	70	86% complied with
2020 **	97	94% complied with
2021	153	96% complied with
2022	No data for Telenor Myanmar for 2022 in Non- financial reporting system as M1 (new owner) took over in March'22	

75. Each of the 153 requests Telenor received in 2021, as well as requests received in 2022, may include multiple users and phone numbers.[39] According to NRK, user data related to 1 300 customers were delivered to the military junta after the coup, and nearly 500 customers risked being arrested if the data were delivered to the junta.[40]

76. While there may be some uncertainty regarding the exact numbers, Telenor has been given the opportunity to comment on the media coverage and has not indicated that the numbers are wrong. Arrests and persecution of opposition leaders that were Telenor customers are also reported to be documented, including opposition leaders that have been arrested and executed. The media reports indicate that Telenor's top management was aware of the specific risks in individual cases, without this being decisive for any decision to comply with the requests.

77. It has not been possible, however, for the NCP to investigate whether Telenor's sharing of user data can be linked to negative human rights impacts in specific cases. As regards the role that requests for user data played – and still plays – in the military junta's persecution of members of the opposition and human rights defenders in Myanmar, the NCP recalls that many actors in the ICT ecosystem contributes to an individual's digital footprint, and finds it probable that historical customer data, provided by Telenor, could have been a "part of a puzzle" for the authorities to enable them to identify and persecute individuals in specific cases.[41]

[39] See Telenor Annual Authority Request Disclosure Report 2021, chapter 6.1 item b. Telenor has confirmed that this is relevant also for Myanmar.

[40] «Fuck off, Telenor!» – Dokumentar. See also among other media reports: NRK avslører: Telenor delte sensitive persondata med militærjunta.

[41] See the Myanmar ICT Eco-system Study – a summary (appended to the Final Statement), page 5: "There are also many other industries that collect, retain, share and use personal information and therefore contribute to individuals' digital footprints (and with the potential for access by State authorities for surveillance purposes)",

78. As of 14 February 2021, Telenor's policy of transparency regarding authority requests was abolished, after it was made clear to Telenor that further disclosures of authority directives could have serious consequences for employee safety.

79. Telenor purchased, imported, installed, tested, and made "ready for use" the intercept technology that the authorities had required. However, Telenor decided to continue refraining from activating lawful intercept even though the military exercised considerable pressure on the company to comply with its demands to activate the equipment. Telenor states that it never activated the lawful intercept equipment, and that this was an important contribution to the protection of Telenor's customers and others against human rights abuses from the military as long as Telenor continued its operations in Myanmar. It must be noted, however, that Telenor has also stated that if Telenor's employees had been threatened, the intercept equipment would probably have been turned on.[42] Furthermore, the intercept equipment was part of the business that was sold to the new owners.

3.1.5 The contractual arrangement with M1 Group, the requirement that M1 Group found a local partner and the possibility of deleting data

80. As far as the NCP is informed, Telenor's contract with M1 Group did not include, and Telenor did not require, contractual terms requiring the buyer to put specific human rights-related policies and procedures in place which could have committed the buyer to operate responsibly in the conflict-affected context that persisted in Myanmar. Telenor has explained that – during its engagements with M1 Group – they highlighted work on sustainability and human rights undertaken by Telenor Myanmar since the start of the Myanmar operations and shared a Responsible Business Conduct framework with M1 before handover. In these dialogues, Telenor explains, M1 Group expressed orally an ambition to continue the work after taking over the ownership of Telenor Myanmar (now ATOM). Telenor has informed the NCP that ATOM's code of conduct includes a section on human rights.

81. Already in November 2021, it was publicly known that it would be a requirement from the junta that M1 Group found a local partner, and that the local partner should be the majority owner.[43] In January 2022, Reuters reported, that several Myanmar firms had expressed an interest in buying Telenor Myanmar's operations and that M1 Group had held talks with Shwe Byain Phyu Group about a partnership. The two firms made a joint proposal to take over Telenor Myanmar and the proposal was accepted by the junta leadership a month later, according to industry sources.[44] The Shwe Byain Phyu Group was publicly known to have

---

but also that one type of data that are regarded as particularly sensitive is "data held by companies that have a physical presence (such as infrastructure, offices and employees) in the country because – as well as jurisdictional considerations – this offers greater leverage to the junta to demand access to this information".

[42] Outcomes of Telenor's internal learning process from the Myanmar engagement, Preamble from Telenor.

[43] Reuters, Telenor sale of Myanmar unit stalls as junta seeks local buyer participation -sources | Reuters, 9 November 2021.

[44] Aftenposten, Telenor-sjefen valgte å følge juntaens ordrer. Her forklarer han hvorfor, 18. mars 2022. It was also in the public domain 21 January 2022, see Reuters article here: Myanmar junta backs Telenor unit sale after buyer M1 pairs with local firm.

close connections to the military junta.[45] Telenor had no contact or dialogue, however, with the local partner and majority owner, Shwe Byain Phyu Group.

82. Telenor explains in its submission to the NCP[46] that deletion of traffic data was thoroughly assessed. One problem was that Telenor's datacentre was located in an area were state of emergency and martial law had been declared. According to Telenor, employees would have been in danger of death penalty and execution without trial if they had deleted data. In addition, purging of such data would have been time-consuming and most likely discovered by the military regime before it was concluded, leaving employees at serious risk. Keeping the data intact was also important for the company's continued operations. Thus, deletion of date was, according to Telenor, not an option.

3.1.6 The situation after the sale of Telenor Myanmar was completed

83. As regards the situation after Telenor's sale of its Myanmar business to new owners was completed in March 2022, the Myanmar ICT Ecosystem Study explains that "[i]n 2024, the different laws relating to surveillance powers are broad and vague in scope in a way that can be used to justify nearly any type of violation of privacy and freedom of expression".[47] Further, it identifies several examples of surveillance of digital footprints:

> "a. It should be assumed that Lawful Intercept (LI) capability is likely active in at least the networks of the four mobile operators. This would mean that, for example, mobile telephony calls, text messages, interception related information (IRI)iv, and device location (by cell tower ID) can be intercepted in real-time. Shutdowns of internet services, which remain frequent in Myanmar, force people to rely on 2G communications, increasing risks from LI facilitated surveillance. It is important to note that LI can also be used to intercept roaming traffic under certain circumstances.
>
> b. It is known that the junta have requested historical data from mobile operators, which can pertain to, for example, subscription data, call detail records and location information. It should be assumed that this and other type of user data is also being requested or accessed from other locally operating digital services, such as digital banking services, VPN or Burmese keyboard apps."

3.2. Limitations in the NCP's factual basis for the examination

84. Throughout the NCP process, Telenor has invoked security concerns as a basis both for their limited possibilities to engage with the complainants at an earlier stage and to share information regarding the sale of the company and other information pertaining to the company's operations in Myanmar, including externally procured security assessments of risks to employees. The concerns underpinning the company's position regarding sharing of information are, as far as the NCP understands, mainly security concerns regarding risks for their employees and sources within Myanmar. Telenor also explains that the risk

[45] Panorama nyheter, Har godkjent salget av Telenor Myanmar, 18. mars 2022.
[46] See Telenor's submission to the NCP of 20 January 2025, page 15.
[47] Myanmar ICT Ecosystem Study – a summary (February 2024), included in Attachment 2.

assessments, including human rights impact assessments and sustainability assessments, in connection with the sale of Telenor Myanmar, were intertwined with communications and other considerations and that sharing them publicly would increase people security risks.[48] According to Telenor, security risks still continue to hinder the company from sharing risk assessments and information regarding e.g. the sale of the business and authority requests prior to the sale.

85. The NCP does not have access to sufficient information to assess the validity of Telenor's security concerns. Moreover, the NCP has made it clear that it cannot receive information that cannot be also shared with the complainants. A deeper insight into the undisclosed risk assessments undertaken by Telenor, which were, as the NCP understands, also based on third-party assessments on the risks to Telenor personnel could possibly have had an impact some of the NCP's assessments. The NCP has, however, taken note of the indications of security risks and risk assessment as far as Telenor has described them in its submissions to the NCP.

3.3. An overview of the basis for the NCP's assessments

86. In light of the limitations described in section 3.2 above, the NCP must base its assessments in the Final Statement on the submission by the parties, the MoU and other publicly available information insofar as it has been shared with the parties for comments and is reliable in the light of all the information made available to the NCP.

87. The NCP has received a human rights impact assessment undertaken by Telenor after the coup and updated as of 18 November 2021, related to two different scenarios: immediate abandonment and insolvency. It should be noted, however, that this human rights impact assessment does not relate to the scenario that was in fact chosen by Telenor, i.e. to sell an ongoing business.

88. As regards the chosen solution, i.e. the sale of the Myanmar business, Telenor provides clear explanations in their submissions to the NCP of their assessments and prioritisation of potential and actual human rights impacts with which the company was involved after the military coup in February 2021. These explanations are the starting point for the NCP's assessment of Telenor's observance of the due diligence expectations in the Guidelines.

89. Moreover, the NCP must build its assessment on the agreed statement in the MoU that all the options considered by Telenor entailed severe human rights risks to customers and to the 734 Myanmar-based employees, as well as risks to local contractors, suppliers and society-at-large. Also, as the parties agree, the NCP builds on the fact that the human rights risks from the sale of Telenor Myanmar became more salient when it was made clear that the regulatory approval was contingent on local ownership. Further, according to the MoU, the Parties acknowledge that as a result of the coup, there are currently more serious risks

[48] See Telenor's submission to the NCP of 20 January 2025, page 8. One of the key lessons learned among the set of learnings published by Telenor in 2023, was that such risk assessments should be documented as standalone so that they can more easily be shared with external stakeholders.

to end users in Myanmar connected to how their information and communications technology can be misused against them by the military junta. The Parties also acknowledge that there still are risks to some former Telenor Myanmar employees such as social and physical punishment for association with the military.

90. The NCP reiterates that the Parties agreed in the MoU that an assessment of the risks to people arising from the decision to sell Telenor Myanmar should prioritise risks based on their severity to people. The Parties disagree, however, on how this is reflected in Telenor's risk prioritisation in the case of Myanmar.

3.4. Issues related to the mediation process

91. The complainants are of the view that Telenor failed to engage meaningfully in the NCP process from the very beginning and throughout the mediation, challenging Telenor's position that it could not participate in the process until it had completed its sale and hence harm was done. According to the complainants, Telenor was dishonest and disingenuous about the buyer and there was a lack of meaningful outcomes from interim agreements.[49] Telenor is of the view that there were positive outcomes of the mediation and collaboration, particularly concerning the ICT Ecosystem Study. They find, however, that the complainants introduced new requirements, outside the scope of the MoU, for entering final mediation.

92. The NCP recalls that preparation for mediation started immediately after the Initial Assessment was published on 27 September 2021. The external mediators were selected before the holidays in December 2021, based on input from, and acceptance by, both parties. Telenor was clearly informed by the complainants about the risks related to the sale to M1 Group, especially the risks related to transfer of user data, and the NCP repeatedly underscored the urgency of the matter in its communication with Telenor.

93. The complainants inquired in December 2021 whether they could have confidence that Telenor would not transfer any user data while the NCP proceedings were ongoing, even if the regulatory approval was granted. It was decided that this issue should be addressed by the mediators, and the parties agreed to proceed accordingly. A pre-mediation meeting was scheduled for January 2022, and a draft mediation framework was prepared by the mediators at the beginning of January 2022. At this stage, the complainants also raised strong concerns regarding the sale of Telenor Myanmar to M1 Group and the local conglomerate, Shwe Byain Phyu Group. Mediation did not commence before June 2022, however, after the sale process was concluded and Telenor's senior management had returned home safely.

94. According to the OCED Guidelines, due diligence is dynamic – it is ongoing, responsive and changing. Through its due diligence process, an enterprise should be able to adequately respond to potential changes in its risk profile as circumstances evolve. The measures that an enterprise takes to conduct due diligence should be commensurate to the severity and

[49] Complainants' observations following failed mediation of 9 September 2024, page 2.

likelihood of the adverse impact.[50] Impacts should be reassessed in response to or in anticipation of changes in the operating environment.[51]

95. Due to the information about the potential transaction between M1 Group and Shwe Byain Phyu Group, Telenor explains that it did conduct an integrity due diligence (IDD) of Shwe Byain Phyu Group, including human rights and sanction issues. The IDD has not been shared with the NCP. This did not, however, change Telenor's assessment that the sale was their only option. Neither did it change Telenor's human rights assessment of the transaction significantly.[52]

96. The complainants held a very different view as from the time it was known that M1 Group had to be joined by a local partner (see paragraph 81). They consider that the sale of the business to a company directly linked to the military regime clearly exacerbated the risks for end users in Myanmar.[53] In the view of the NCP, it is true, as indicated by Telenor, that any new owner had to comply with the laws of Myanmar and would probably be forced to comply with orders of the military junta. A majority owner with close ties to the military junta would probably also be inclined to more actively support the aims of the authorities and, in any event, not be interested in offering any mitigating measures to customers or supporting efforts to improve the security of end users, including targeted individuals. In this regard, it should be noted that Telenor's original justification for the sale to M1 Group – that this would secure a fourth *independent operator* in Myanmar[54] – no longer held true. As mentioned above (see paragraph 22), the parties agreed in the MoU that the human rights risks from the sale of Telenor Myanmar became more salient when it was made clear that the regulatory approval was contingent on local ownership.

97. This change of circumstances should have triggered a renewed human rights risk assessment and thorough human rights due diligence process of the sale, including a renewed prioritisation of risks to employees, Telenor's customers and others. All possible options to mitigate risks also to end users should have been included in the human rights due diligence process at this stage. In general, an IDD of the local partner falls short of this.

98. Furthermore, meaningful engagement with rightsholders, potentially affected groups and other relevant stakeholders is an essential element of human rights due diligence in conflict-affected situations.[55] The NCP recalls that the complainants comprised Myanmar organisations and individuals who could be directly affected by the risks pertaining to the sale of Telenor Myanmar and, among other things, the transfer of user data to the military junta . On the other hand, engagement with stakeholders may be restricted by e.g. rules of confidentiality pertaining to mergers and acquisitions processes.[56]

---

[50] See OECD (2018), OECD Due Diligence Guidance for Responsible Business Conduct, page 17.
[51] L.c. page 26 (point 2.2 item g).
[52] See Telenor's submission to the NCP of 20 January 2025, page 9.
[53] See also SOMO's submission to the NCP of 31 January 2025, page 2.
[54] Telenor's response to the complaint of 12 August 2021.
[55] See Shift (2015). Human Rights Due Diligence in High Risk Circumstances: Practical Strategies for Businesses, page 15.
[56] There are certain difficulties associated with conducting human rights due diligence in relation to mergers and acquisitions, as such processes are normally guarded by an elevated level of confidentiality for legal and

99. The NCP reiterates that Telenor failed to use this opportunity to, as far as possible after the sale was announced, reassess its risk-assessment, prioritizations and human rights due diligence at a critical point in time based on dialogue with important rightsholders and possible victims of the junta's persecution of the opposition and others. This could have informed possible actions by Telenor to mitigate such risks.

100. On the other hand, the NCP finds that the parties, from the start of the mediation in June 2022, addressed key issues raised in the complaint in the dialogue facilitated by the mediators. The NCP commends the parties for also agreeing to publish the MoU, which clearly summarizes points of agreement and disagreement, and includes specific follow-up actions and key issues for further discussion. In particular, the ICT Ecosystem Study identifies privacy and surveillance risks for users in Myanmar and other high-risk, conflict-affected areas that may be useful beyond this Specific Instance. The NCP also commends Telenor for reviewing risk assessments conducted at the time and discussing lessons learned with a broader stakeholder group.

101. The NCP has reviewed the statements from both parties as well as the outcomes, finding that meaningful progress was made during the mediation on some aspects of the Specific Instance (see sections 2.5 and 2.6). Nevertheless, the parties had diverging views on key issues; notably the nature of Telenor's involvement in adverse impacts and Telenor's responsibility to provide for remediation through a digital security relief mechanism.

102. Despite the initial delays in Telenor's engagement in the NCP process described and commented above, as well as Telenor's failure to fully reassess the risk assessment, prioritisation and human rights due diligence, the NCP does not – taking into account the challenging situation in Myanmar at the time and the security concerns that Telenor invoked – have sufficient reason to conclude that either party failed to participate in the mediation in good faith.

103. As regards Telenor's complaint that SOMO breached its duty of confidentiality in its statements to the media about the mediation in August 2025 (see paragraph 44), the NCP recalls that Parties to a mediation agree on abiding by the confidentiality provisions in the Guidelines and the framework for mediation. Information exchanged during the process is to remain confidential. Parties are nevertheless free to disclose their own information as long as this does not include information that belongs to the other party.

104. SOMO is quoted in NRK on 31 August 2025 as saying that Telenor rejected a digital relief mechanism and had sent a clear message that they would not pay a cent to such a mechanism. The NCP cannot confirm whether this refers to actual statements from Telenor during the mediation, and this is disputed by SOMO. The NCP does not find reason to investigate this further but notes that the statements do not contribute to a constructive dialogue, especially in the light of Telenor's repeated statements that the company remains committed to continuing its engagement to explore a digital relief mechanism.

---

other purposes. The NCP has recently addressed the issue of stakeholder engagement in the context of M&A processes, see for instance paragraph 72 in the Final Statement Pax and others vs. Aker BP and Aker ASA.

3.5. Examination of remaining issues

3.5.1 Did Telenor carry out risk-based due diligence, including stakeholder engagement and communication, in line with the Guidelines, in relation to the disengagement from Myanmar?

105. Human rights due diligence must be risk-based and identify and address the most serious actual and potential risks. The due diligence should be commensurate to the severity and likelihood of the adverse impact. It is well established that the most serious risks are found in conflict-affected areas. Through the due diligence process, an enterprise should be able to adequately respond to potential changes in its risk profile as circumstances evolve. These basic principles applied to Telenor's due diligence efforts throughout its operations in Myanmar.

106. At the outset, it should be recalled that Telenor decided to integrate assessments of human rights risks, including risk to employees, customers and other rightsholders into the overall and operational crisis management that was established after the military coup. This is compatible with the Guidelines, as "[h]uman rights due diligence can be included within broader enterprise risk management systems, provided that it goes beyond simply identifying and managing material risks to the enterprise itself to include the risks to rights-holders".[57]

107. Based on the examination of Telenor's actions prior to and following the coup, the NCP finds that serious human rights risks were identified and that some of them were effectively mitigated. The NCP agrees that protecting the lives and security of the company's employees is a core component of the corporate responsibility to respect human rights. Prioritizing employee safety, however, does not absolve a company of the responsibility to seek to mitigate the risks for customers and other rightsholders. The NCP has no reason to doubt that Telenor also had a clear understanding of the risks to customers and to other rightsholders.

108. The Human Rights Impact Assessment (HRIA) (November 2021), see paragraph 87, assessed the two scenarios of immediate abandonment and insolvency, whereas neither of these options were chosen. It should be mentioned, however, that some of the risks – risks to employees, customers, suppliers and society at large – identified in the HRIA were in fact avoided when Telenor decided to sell an ongoing business instead of immediately abandoning the business.

109. In relation to the option to sell an ongoing business, Telenor has explained that the company, when deciding to exit Myanmar, assessed both the risks that it was involved in and Telenor's ability to mitigate risks. Shortly after the coup, Telenor decided to prioritise the following:

    - First and foremost, ensure personnel safety and security;
    - Ensure continued network availability for the customers;

[57] OECD Guidelines (2011) Part I, Chapter IV. Human Rights, paragraph 45.

- Stay transparent to the extent possible when handling orders from the military and on developments on the ground in Myanmar;
- Safeguard the operations.[58]

110. This list was followed throughout Telenor's remaining operations in Myanmar. Personnel safety and security remained the top priority. Priority was also given to ensuring network availability and safeguarding the operations. It was not, however, according to Telenor, possible for the company to stay transparent, mainly due to the risk to the security of the company's employees, see paragraph 78 above.

111. The abovementioned priority list makes it clear that the safety and security of Telenor's customers was not – under the circumstances – a prioritised risk for Telenor. In practice, Telenor complied with all the military junta's requests for historical user data after the coup, see paragraph 74 above. Further, Telenor explains that the junta prohibited public communication regarding authority requests, and that it thus became impossible for the company to communicate with its customers as before, and the company could no longer be transparent when handling orders from the military. Also, Telenor did not delete any of the user data that were stored in Myanmar, and this was eventually transferred to the new owners as part of the sale, together with the lawful intercept equipment.

112. Telenor explains that commitment to human rights was a key factor in prioritizing the risks and mitigation efforts, and that the heightened risk of human rights violations was duly acknowledged in the risk assessments and prioritisation. However, the company's possibilities to undertake due diligence, including opportunities to mitigate risks to employees and customers, seem to have been more limited in the post-coup context than before. The result was that Telenor chose – in practice – to follow a general rule; no employee should have to risk their life or health – and employee safety was always put first. This was done, it seems, in spite of the known risks of persecution of individual customers targeted by authority requests.

113. The NCP acknowledges that serious security risks for employees became a reality for Telenor after the coup and when military rule was reintroduced in Myanmar. The NCP also appreciates that this necessarily made the company's room of manoeuvre narrower due to threats and oppression from the military, as well as from other groups. The possibility to build leverage over the authorities, including in cooperation with others, must clearly have been more limited than before the coup.

114. Furthermore, the NCP has no reason to question the gravity of the dilemmas and severity of the security challenges the Telenor faced. Human rights due diligence must, however, be dynamic and risk-based. Human rights due diligence "is an on-going exercise, recognising that human rights risks may change over time as the enterprise's operations and operating context evolve".[59] Moreover, prioritisation shall be risk-based, and guided by the severity and likelihood of the actual or potential adverse impact. When the likelihood and severity of the

[58] Submission from Telenor to the NCP of 20 January 2025, page 5.

[59] See the OECD Guidelines (2011), Part I, Chapter IV. Human Rights, paragraph 45.

impacts is high, due diligence should be more extensive. This is especially important in CAHRAs, like Myanmar was both before and after the military coup.

115. In the case of Telenor's disengagement from Myanmar, it seems improbable to the NCP that the risks to the company's employees in all circumstances and at all times outweighed and restricted mitigation efforts in regard of other human rights risks with which the company was involved. In other words, the company's risk assessment and prioritisation must be part of a more holistic due diligence process so that the risks to employees are being weighed against the risks for other groups, which may vary over time and in different contexts, and, moreover, be assessed in the light of the real risks created by the range of available mitigating efforts for other at-risk groups, or even other individuals in concrete cases. However, in Telenor's assessments, the health and safety of employees always came first. In the view of the NCP, it was not in accordance with the expectations of Guidelines to systematically give priority to one set of rightsholders, i.e. Telenor's own employees.

116. The recommendations to all ICT companies operating in CAHRAs in the Myanmar ICT Ecosystem Study[60] are helpful in establishing a reference point for the assessment of Telenor's due diligence with regards to its disengagement from Myanmar. The Study includes, among others, the following recommendations:

- Ensure that country-level human rights impacts assessments are informed by the perspectives and expertise of rights-holders from the country in question.
- Transparently communicate the findings of human rights due diligence processes (HRDD) and the actions taken to prevent and mitigate risks as a result of those findings.
- Include human rights considerations and exit scenarios within the company's crisis management planning and regular crisis exercises with a particular focus on operations in CAHRAs.
- Conduct dynamic and enhanced human rights due diligence in relation to operations within CAHRAs, including designing processes for rapid HRDD for complex and fast evolving situations and identifying most at-risk and vulnerable rights-holders.
- Proactively identify ways in which the company can support users' digital safety and security generally and in relation to the specific circumstances facing users in CAHRAs through, for example:
  - offering services and features that support digital safety and security (examples include Nord VPN's free emergency VPN offer and Facebook's safety feature enabling users to quickly and easily lock their profiles.);
  - supporting wider initiatives to build digital safety and security understanding amongst users, in particular those rights-holders at greatest potential risk;

[60] See the Myanmar ICT Ecosystem Study – a summary (appended to the Final Statement), page 7-8.

- providing financial and material support to civil society and academic research that aims to build understanding and highlight human rights abuses using ICT;
- putting in place operational level grievance mechanisms that would allow at risk persons to both make contact and securely communicate with the company, and access individual remedy.

117. Even if these recommendations are formulated after the events in this Specific Instance, they illustrate typical actions available to ICT companies operating in CAHRAs in their efforts to handle and mitigate risks that they may be linked to. It must be appreciated, however, that e.g. fully transparent communication may be difficult, or even impossible, in a conflict situation, but also that there, in most cases, are possibilities for confidential communication when stakeholder relationships are already established.

118. As indicated above, in paragraph 115, Telenor's human rights due diligence should have assessed whether the risks to Telenor's employees in all cases necessarily prevented *any efforts* by the company to prevent and mitigate adverse impacts for other at-risk individuals, including its customers, related to the company's sharing of user data with the junta. The NCP does not have evidence, however, that Telenor undertook any such efforts, considered to do so nor had dialogue with rightsholders in order to get advice on how to do so. In its submissions to the NCP, Telenor only states, on a high level, that they conducted ongoing and dynamic human rights due diligence and impact assessments and took steps to mitigate impacts, without specifying or indicating the impacts they disclosed nor any mitigating efforts that were made in relation to the sharing of data with the junta.

119. Moreover, the human rights risks became more salient when it was known that the Myanmar authorities required that M1 Group found a local partner as majority owner. This should have triggered a new, thoroughgoing human rights due diligence process and reassessment of prioritisation of risks pertaining to the sale of the company, see paragraph 89 above. As far as the NCP is informed, this was not done.

120. As regards measures to help customers to protect their communications, Telenor explains in its submission to the NCP that an operative mobile network made it possible for people in Myanmar to communicate also through use of VPN and encrypted services, such as Signal and WhatsApp, and that they had the clear impression that people in Myanmar started to use such services. Furthermore, it is mentioned in Telenor's submission to the NCP that Telenor Myanmar informed customers about how to use the internet safely.[61] It is unclear, however, to what extent this provided helpful information to customers about how they should protect themselves from misuse of authority requests for information, typically historic user data.[62]

[61] See Telenor's submission to the NCP of 20 January 2025, pages 5-6. A more detailed account for the programs and their outreach is found in Telenor's comments on the draft Final Statement 19 November 2025.
[62] Programs for online security prior to the coup mainly dealt with tolerance and respect and the dangers of hate speech, see Telenor's Sustainability briefing 2020. The programs described in Telenor's comments to the Final Statement of 19 November 2025 seem also to be of a more general nature, and Telenor does not state that they addressed especially the surveillance risks and at-risk customers' need to protect their user data from misuse by the authorities.

121. The complainants take issue with Telenor's assessments and state that Telenor could have mitigated the risks related to the sale of the company if it had informed users about the risks to their security and possible steps they could take to mitigate those risks. According to the complainants – i.e. a large group of local civil society actors comprising many of those at risk in Myanmar – "[m]any users, including civil society activists, did not, and still do not, know the content of the data that has been collected by Telenor" and that "[t]his lack of clarity makes it difficult for them to assess their levels of risks following the data transfer".[63] Thus, the complainants argue that Telenor should have provided material and technical support to users to help mitigate individual risks following the sale. The ICT Ecosystem Study confirms this need, noting that "[a]lthough human rights defenders (HRDs) are increasingly aware of the risks relating to digital footprints and the steps they can take to help to reduce risks to their safety and security, many lack the resources to be able to use all technical safeguards available", see paragraph 36 above. Based on the available information, the NCP concludes that Telenor did not provide its customers with information or training on how they should protect themselves from misuse of authority requests for information, typically historic user data – neither before the coup nor after. At-risk customers were, as far as the NCP is made aware, not provided with any form of assistance. In the view of the NCP, Telenor should have included the possibility of such support to customers in their on-going human rights due diligence, and carried out support, especially to at-risk customers, whenever possible.

122. As regards its engagement with stakeholders, Telenor states that the company had extensive dialogue with stakeholders throughout the operations in Myanmar. This also includes at least 125 calls/meetings concerning the human rights situation in Myanmar in 2021, and at least 36 in 2022. According to Telenor, these were calls and meetings with, among others, civil society organisations within and outside Myanmar. A core element of the complaint is, however, that Telenor neither consulted nor engaged with any of the 474 Myanmar-based CSOs supporting the complaint.[64] The NCP builds on this information, and has not received any specific information suggesting that Telenor consulted with potentially affected rightsholders or directly affected groups or individuals in Myanmar. Further to this, Telenor's delayed engagement with the complainants in the mediation until the sale was completed and foreign employees had returned home safely (see paragraph 93) indicates a more general reservation from engaging with these groups.

123. Dialogue with a broader group of stakeholders could have provided Telenor with input on how to mitigate risks for customers. While more challenging in conflict contexts, such engagement is only more important in moments of crisis and confidential dialogues are in most cases still possible. In the view of the NCP, Telenor's human rights impact assessments should have been informed by the perspectives and expertise of rightsholders and directly affected groups and individuals in Myanmar. This was not done.

124. The NCP underscores that the human rights due diligence undertaken by Telenor after the coup cannot be assessed in isolation. To understand and assess Telenor's handling of risks after the coup, it is necessary to take into account that Telenor was not prepared for the

[63] See SOMO's submission to the NCP of 31 January 2025, page 8.
[64] See SOMO's complaint to the NCP of 27 July 2021, pages 9-10.

situation created by the military coup in February 2021, see paragraph 70. As a result, the company's ability to mitigate risks for all those who were seriously at risk of persecution or reprisals were most likely more limited than it would have been if Telenor had been prepared for a scenario with full military rule in Myanmar and/or a scenario where Telenor was forced to exit the country due to pressure from the Myanmar authorities. It follows from Telenor's submissions to the NCP that e.g. being forced to activate lawful intercept was "a red line" for the company, and – especially in the light of mounting pressure from the authorities prior to the coup a forced exit was thus not an unrealistic scenario for Telenor.

125. Many of the efforts to mitigate risks for end users, e.g. as illustrated in the recommendations cited in paragraph 116 above, should have been implemented, or prepared for, before the coup. As far as the NCP is informed, this was not done.

126. In sum, Telenor did not undertake human rights due diligence commensurate to the severity and likelihood of the adverse impacts with which the company was involved in in Myanmar.

3.5.2 Should Telenor play a role in remediation of adverse impacts, and if so, what role would be appropriate?

127. The main responsibility for the grave human rights violations in Myanmar lies with the military junta. The state duty to protect human rights is established in international human rights law. It is reflected in the OECD Guidelines and is the first of the three pillars in the UN Guiding Principles on Business and Human Rights.

128. Businesses have a duty to respect human rights. This means that they should avoid infringing on the human rights of others and should address adverse human rights impacts with which they are involved. This duty is duly established in the Guidelines and aligned with the UN Guiding Principles for Business and Human Rights.

129. An enterprise's role in remediation under the Guidelines depends, at the outset, on how it is linked to adverse impacts. Enterprises are expected to provide for or cooperate in remediation when they have caused or contributed to adverse impacts. When they are directly linked to such impacts, they are encouraged to take a role in remediation but are not called on to provide for it directly.

130. The NCP reiterates that the assessment of the enterprise's involvement with a potential or actual negative impact must be based on the facts of each case. This assessment under the Guidelines is not a legal assessment, and it does not include the issue of intent or culpability. The Guidelines are voluntary and remedial rather than binding and punitive. The Guidelines do not create or define liability for enterprises. Rather, they seek to encourage the positive contributions enterprises can make to economic, environmental, and social progress and to minimise adverse impacts.[65]

131. In this case, the complainants claim that Telenor contributed to negative impacts for its employees, customers and society-at-large through the exit from Myanmar. According to the Guidelines, a company's contribution must be substantial to fall within this category,

[65] OECD Guidelines (2011), Preface.

meaning that it does not include minor or trivial contributions. The following factors may be taken into account:

- The degree to which the activity increased the risk of the impact occurring;
- The degree of foreseeability, and
- The degree to which any of the enterprise's activities actually mitigated the adverse impact or decreased the risk of the impact occurring.

Moreover, the mere existence of a business relationship or activities which create the general condition in which it is possible for adverse impacts to occur does not necessarily represent a relationship of contribution. Under the Guidelines, the activity in question should substantially increase the risk of adverse impact.[66]

132. The NCP's examination of the Specific Instance does not include assessments of whether Telenor's actions – e.g. complying with the junta's requests for user data – have contributed to negative impacts in individual cases. As mentioned above in paragraph 77, user data provided by Telenor could have been "part of the puzzle", but not necessarily decisive, nor even necessary, for the military junta's persecution in individual cases. Thus, it remains undecided by the NCP whether, and to what extent, Telenor's activities increased the risk of negative impacts in individual cases.

133. In general, however, provision of user data to a military junta that uses the data for surveillance of political opponents may be regarded as contribution to adverse human rights risks and impacts.[67] It was foreseeable that the military junta could misuse requested user data and violate Telenor's customers' human rights, e.g. the end users' right to privacy, freedom of expression and violations due to other types of persecution. Moreover, Telenor's activities did not decrease the risk of adverse impacts occurring. After the coup, Telenor was unable to restrict the transfer of user data to the military junta, and the company's prioritisation of employee security trumped, as explained by Telenor, nearly any possible actions to mitigate the risks for end users. On the other hand, Telenor was required by local law to comply with the requests, and after the coup the requests were supported by threats of serious harm to Telenor's employees.

134. Under the OECD Guidelines, as well as under the UN Guiding Principles on Business and Human Rights, there is a continuum between contribution and linkage.[68] These categories may not necessarily be seen as rigid categories, but rather as "guiding principles" designed to assist companies in assessing how they can act responsibly.[69] This is illustrated by the Follow Up Statement by the Australian Contact Point published 27 February 2020.[70] In this

[66] OECD (2018), OECD Due Diligence Guidance for Responsible Business Conduct, Annex, Q29.
[67] See The Danish Institute for Human Rights, Phase 3: Analysing Impacts, Human Rights Impact Assessment Guidance and Toolbox, page 6.
[68] See Ruggie, John G. (2017). Comments on Thun Group of Banks Discussion Paper on the Implications of UN Guiding Principles 13 & 17 In a Corporate and Investment Banking Context.
[69] See Business for Social Responsibility (2021), Seven Questions to Help Determine When a Company Should Remedy Human Rights Harm under the UNGPs.
[70] Follow Up Statement Regarding complaint submitted by Equitable Cambodia and Inclusive Development International on behalf of Cambodian families, 27 February 2020.

Specific Instance – like in our Specific Instance – another actor than the respondents was primarily responsible for the alleged harms. Paragraph 8 reads:

> "Where a company's due-diligence identifies impacts which it has caused or contributed to, or to which it is linked through a business relationship, the company has responsibilities regarding remedy for those impacts. Where a company has gained revenue in a manner inconsistent with the OECD Guidelines, and that has resulted in parties being impacted, the payment of the revenues to those parties may be one way a company can comply with the requirements of the OECD Guidelines."

135. Also in our case, it is not necessary to identify exactly where on the continuum between contribution and linkage the Specific Instance sits. In any event, a company's responsibility to provide for or to participate in remediation is determined by the nature and extent of its contribution to the harm. It is also expected to use and build leverage to ensure that the other responsible parties play a role in remedy too.[71] Importantly, the mediation process and the MoU indicate that Telenor has accepted to take a role in the remediation of adverse impacts, especially by funding the ICT Ecosystem Study, and committing to follow up this study by exploring how an independent Myanmar digital relief mechanism could be established and to provide support (financial and other) to Myanmar citizens facing risks and impacts associated with their digital footprint, see paragraph 36 above. In its final submission to the NCP, Telenor reiterates that it is committed to supporting wider initiatives to build digital safety and security understanding among ICT users, and to explore what options there are for Telenor to engage in it. The NCP considers these commitments, which are forward-looking and relevant in addressing future risks created by the sale of Telenor Myanmar, commensurate to the nature and extent of Telenor's contribution to the adverse impacts.

136. Thus, Telenor is expected to take an active role in remediation to the extent of its contribution by further follow-up of the commitments in the MoU. Telenor is furthermore expected to cooperate in the remediation, as a key telecommunications operator, within a broader remedy ecosystem.

4. Conclusions

137. Some serious human rights risks were identified and mitigated through Telenor's human rights due diligence in relation to its disengagement from Myanmar. Protecting the lives and security of employees is indeed a core component of the corporate responsibility to respect human rights.

138. Telenor did not, however, undertake ongoing human rights due diligence commensurate to the severity and likelihood of the adverse impacts with which the company was involved in in Myanmar; it was not in accordance with the expectations of Guidelines to systematically give priority to one set of rightsholders, i.e. Telenor's own employees. Telenor's human rights due

[71] See e.g. Human Level (2023). Study on Access to Remedy for Workers in the Context of the FIFA World Cup Qatar 2022, page 17.

diligence systematically gave lower precedence to engagement with other rightsholders, e.g. measures to help customers protect their communication, and risk-based prioritisation of impacts with which the company actually or potentially were involved. The human rights due diligence was therefore not as dynamic and risk-based as the Guidelines expect. Any consequences of this in individual cases have not been examined by the NCP.

139. Telenor's human rights due diligence after the coup was furthermore limited by the fact that the company's ability to mitigate risks for all those who were seriously at risk of persecution or reprisals most likely was more limited than it could have been if the company's human rights due diligence prior to the coup had encompassed the possibility of reintroduction of full military rule in Myanmar and a forced exit from the country, with corresponding human rights due diligence based on exit scenarios.[72]

140. A new, thoroughgoing risk-assessment, human rights due diligence and reassessment of prioritisation of risks pertaining to the sale of the company should have been undertaken when it became clear that the Myanmar authorities required that M1 Group found a local partner as majority owner.

141. Telenor's contract with M1 Group should have gone beyond simply ensuring that the company expressed an ambition to respect human rights. Telenor should at least have required that the buyer put specific human rights-related policies and procedures in place to commit them to, as far as possible, operate responsibly in a conflict-affected context.

142. The NCP expects Telenor to take an active role in remediation to the extent of its contribution to adverse impacts by further follow-up of the commitments in the MoU, notably through a digital relief security mechanism. Telenor is furthermore expected to cooperate in the remediation of adverse impacts, as a key telecommunications operator, within a broader remedy ecosystem.

5. Lessons learned and recommendations from the NCP

143. A key lesson learned from this Specific Instance is the importance of carrying out risk assessments and human rights due diligence processes that encompass scenarios for responsible exit, both when entering markets recovering from military rule and in other fragile, post-conflict settings.

144. The NCP recalls that Telenor's entry into Myanmar was marked by a high degree of optimism – not least by the Norwegian government – and yet also some sobriety. Telenor made numerous efforts to work for an improvement of the regulatory framework, as well as to prevent and mitigate adverse human rights impacts. A fundamental risk, however, was absent from the assessments: the real risk of being forced to leave Myanmar, e.g. because of

[72] The NCP has not found it necessary to make a final *determination* on the question of whether the Guidelines strictly required Telenor to have in place an exit strategy at the time of entry or later during its operations in Myanmar. On the other hand, this is today an established and recommended part of heightened human rights due diligence in high-risk areas, and the NCP has therefore included in its *recommendations* that Telenor integrate exit strategies in its due diligence prior to entering new markets, based on the findings and lessons learned in this Final Statement.

mounting pressure to activate lawful intercept and/or due to Myanmar reverting to full military rule. The absence of focus on this risk in Telenor's human rights due diligence is striking in hindsight. The risk was not considered, and Telenor had no exit strategy. Exit strategies were made and analysed only after the risks had become a reality.

145. Contrary to the set of learnings from Telenor cited above in paragraph 69, the NCP is of the opinion that human rights due diligence processes prior to the coup, including responsible exit considerations based on a realistic assessment of a scenario where full military rule was reintroduced in Myanmar, would have made a difference. In general, this finding is supported by the recommendation in the Myanmar ICT Eco-system Study to "include human rights considerations and exit scenarios within the company's crisis management planning and regular crisis exercises with a particular focus on operation in CAHRAs". This recommendation has strong support in authoritative guidance on human rights due diligence in conflict-affected contexts, like UNDP's 2022 Guide[73] and the advice on responsible exit, published by the Office of the High Commissioner of Human Rights in 2023:

> "To the extent possible, business enterprises should plan in advance and have contingency plans in place to provide time to make informed, responsible decisions. While challenging contexts and business relationships may arise suddenly, the risks that a situation may become challenging may be known well in advance. Businesses are too often insufficiently focused on broader operating environments, particularly in planning for operational changes, including potential exit, especially where there has been a "headlong rush into … new markets."
>
> Early planning – at the start of operations or a business relationship, and certainly at the first indications of possible conflict – should make business enterprises better placed to react quickly should the worst happen, for instance through activation of action plans that have been pre-agreed with service-providers, or pre-arranged compensation packages (e.g. for employees) and transition arrangements designed to minimise human rights-related risks (…). This should help to avoid unaddressed adverse impacts when a relationship is ended, as well as any adverse impacts as a result of terminating the relationship".[74]

146. Human rights due diligence prior to the coup, including responsible exit considerations based on a realistic assessment of a scenario where full military rule was reintroduced in Myanmar, would have allowed Telenor to identify and assess in advance the short- and longer-term human rights risks of disengagement, including for members of the opposition and other vulnerable groups. Telenor could then have been better prepared to minimise harmful human rights impacts to all groups that would be at risk after the return to military rule, e.g. by developing at the earliest stage, i.e. preferably at the time of the company's entry to the country, a broader set of mitigation strategies based on stakeholder

[73] United Nations Development Programme (2022). Heightened Human Rights Due Diligence for Business in Conflict-Affected Contexts: A Guide. New York, United States of America.
[74] United Nations Office of the High Commissioner for Human Rights (2023). Business and Human Rights in Challenging Contexts: Considerations for Remaining and Exiting.

engagement as well as building institutional capacity, preparedness and training on heightened human rights due diligence.

147. Possible strategies and mitigation efforts at an earlier stage could have included awareness building among customers, assessing opportunities for minimising stored data, and exploring ways to protect local employees by building leverage over the military together with other companies and actors, and thus create room for also protecting customers and others at risk from negative human rights impact linked to the authorities' request for information and to the sale of the company. In addition, well prepared evacuation strategies, communication strategies and adaptation of the company's decision-making processes to minimise risks for local employees as well as others at-risk individuals could have been included in an exit strategy.

148. The NCP furthermore finds that stakeholders in this Specific Instance were not consulted on options for responsible disengagement. The OECD Due Diligence Guidance (2018) calls on companies to consider and address the potential adverse impacts of a decision to disengage, escalation measures for disengagement and highlights the importance of providing sufficient notice of disengagement.

149. The NCP recommends Telenor to use the lessons learned to integrate exit strategies in due diligence prior to entering new markets, as well as continually updating due diligence, taking into account the need for data protection and stakeholder engagement in volatile and changing political contexts.

150. In particular, the NCP recommends Telenor to continue its engagement and commitment to explore, concretise, design and implement a Myanmar digital security relief mechanism to provide support (financial and other) to Myanmar citizens facing risks and impacts associated with their digital footprint, and thereby cooperate in the remediation of adverse human rights impacts, in line with the conclusions in this Specific Instance. This may be done in cooperation with other actors linked to ICT-related impacts in Myanmar and the region.

6. Follow-up by the NCP

151. The Final Statement will be published on the website of the NCP and submitted to the OECD for publication in the database of Specific Instances.

152. The NCP welcomes any initiative from the parties to continue the dialogue with a view to following up outstanding issues in the MoU, notably when it comes to a digital security relief mechanism.

153. In accordance with the NCP case-handling procedures, the NCP will invite each of the parties to a follow-up meeting within a year after the Final Statement is published to provide the NCP with an update on implementation of the recommendations and any other activities relevant to the issues raised. The NCP will then publish a follow-up statement.