

To Norges Bank

29 June 2023

UNOFFICIAL TRANSLATION

Recommendation to exclude Sumitomo Corp
from investment by the Norwegian Government
Pension Fund Global (GPFGB)

Summary

The Council on Ethics recommends that Sumitomo Corp (Sumitomo) be excluded from investment by the Government Pension Fund Global (GPF) due to an unacceptable risk that the company is contributing to serious violation of the rights of individuals in situations of war or conflict. Sumitomo is a Japanese conglomerate with manufacturing and trading activities within six business areas, one of which is media and digital services. This recommendation relates to the company's telecommunications business in Myanmar.

At the close of 2022, the GPF owned 1.38 per cent of Sumitomo's shares, worth USD 288.4 million. Sumitomo is listed on the Tokyo Stock Exchange.

On 1 February 2021, the armed forces in Myanmar staged a military coup. Since the coup, the armed conflicts taking place within the country have intensified. The UN High Commissioner for Human Rights has stated that the armed forces' actions could qualify as crimes against humanity and war crimes. Assaults on the civilian population are ongoing and well-documented, and there is a substantial risk that the military will commit new, extremely serious abuses.

In Myanmar, Sumitomo is a partner in a joint venture that has signed a joint operation agreement with Myanmar Posts and Telecommunications (MPT). MPT is one of four telecommunications operators in Myanmar. Through the joint venture, Sumitomo has provided expertise and advice in the field of sales and marketing, as well as the expansion of the telecommunications network. Since the coup, MPT has been under military control.

It has been reported that MPT and other telecoms operators in Myanmar have been ordered to install and activate spyware and surveillance software that enable the regime to monitor customers' phone and internet use in real time. In this way, the regime can listen into conversations, read text messages, monitor internet and email traffic, and track the location of users. The level of surveillance has intensified since the coup.

It is not known how data from MPT is used by the police and armed forces. However, it is known that such monitoring has enabled serious norm violations. This includes the arrest of those opposed to the regime on the basis of information obtained through surveillance. MPT's surrender of personal data constitutes a considerable risk to the civilian population and infringes the individual's right to liberty, safety and freedom from torture, as well as the right to a private life and freedom of expression. When assessing Sumitomo's contribution to norm violations, the Council attaches importance to the fact

that the company is engaged in a business association with a partner that enables serious and systematic violations of human rights and humanitarian law. Although Sumitomo plays no direct role in the surveillance, the Council presumes that the company is aware that MPT has installed and activated tools for the political monitoring of human rights activists, political opponents and other individuals.

In its dialogue with the Council, Sumitomo has asserted that it has performed due diligence assessments, that it continuously assesses the human rights situation in the country and that it has attempted to use its influence to address the risk of human rights violations relating to the surveillance. Although this is positive, the company's efforts have borne little apparent fruit. Sumitomo has elected to remain in Myanmar out of concern for its own employees and to help maintain the telecoms infrastructure and communications capacity. The Council acknowledges that the choice between remaining in the country and pulling out represents a potential dilemma for the company and that it has limited freedom of action in its partnership with MPT. Nevertheless, the Council considers that this cannot be accorded decisive weight when there is a considerable risk that MPT will continue to surrender customer data that will enable serious abuses to be perpetrated on the civilian population. While the military holds power in the land, it is unlikely that Sumitomo will wield sufficient influence to prevent this. The Council concludes, therefore, that as long as Sumitomo's partnership with MPT persists, the risk of the company contributing to the violation of the rights of individuals in situations of war or conflict will remain at an unacceptable level.

Contents

Summary

- 1 Introduction 1
 - 1.1 Matters assessed by the Council on Ethics 1
 - 1.2 Sources 3
- 2 Background..... 3
 - 2.1 The situation in Myanmar 3
 - 2.2 Myanma Posts and Telecommunications (MPT)..... 7
- 3 Sumitomo’s business partnership with MPT 8
- 4 Surveillance and control of MPT’s customers 9
- 5 Information from the company 11
- 6 The Council’s assessment..... 13
- 7 Recommendation..... 14

1 Introduction

The Council on Ethics for the Norwegian Government Pension Fund Global (GPF) has assessed the Fund's investment in Sumitomo Corp¹ (Sumitomo) against the Guidelines for Observation and Exclusion of Companies from the Government Pension Fund Global (ethical guidelines).² This recommendation relates to the company's telecommunications business in Myanmar.

Sumitomo is a Japanese conglomerate with manufacturing and trading activities within six business areas, one of which is media and digital services. The largest business area relates to mineral resources, energy, chemicals and electronics. The company has almost 900 subsidiaries, 75,000 employees and operations worldwide.³

Sumitomo is listed on the Tokyo Stock Exchange. At the close of 2022, the GPF owned 1.38 per cent of Sumitomo's shares, worth USD 288.4 million.

1.1 Matters assessed by the Council on Ethics

The Council on Ethics has assessed the GPF's investment in Sumitomo against section 4(b) of the ethical guidelines, pursuant to which: "Companies may be excluded or placed under observation if there is an unacceptable risk that the company contributes to or is responsible for: [...] serious violations of the rights of individuals in situations of war or conflict."

This recommendation relates to the company's collaboration with the Myanmar state telecoms company MPT and the risk of contributing to serious human rights violations as a result of the surveillance of telecommunications traffic in the country. Sumitomo and the company KDDI Corp are partners in the joint venture KDDI Summit Global Myanmar Co Ltd, which has a Joint Operation Agreement with Myanmar Posts and Telecommunications (MPT).

In the Council's opinion, any assessment of whether the risk of a company contributing to norm violations is acceptable or not must be performed in light of the kind of norm violations it risks contributing to. In cases where the company operates in a context where there is a known risk of contributing to extremely serious norm violations, the

¹ Issuer ID: 114805

² Guidelines for Observation and Exclusion of Companies from the Government Pension Fund Global (GPF), https://www.regjeringen.no/contentassets/9d68c55c272c41e99f0bf45d24397d8c/2022.09.05_gpf_guidelines_observation_exclusion.pdf

³ Sumitomo Corporation website, <https://www.sumitomocorp.com/en/jp>

Council takes the position that companies which do business in such areas must be particularly prudent in their exercise of due care. Such a heightened requirement for due care follows from several international guidelines.⁴ It is also reiterated in the Report to the Storting (white paper) on the Government Pension Fund for 2021 (Meld. St. 24 (2020–2021))⁵ and underpins several recommendations previously issued by the Council under this criterion.⁶

When assessing what may constitute serious violations of the rights of individuals in situations of war or conflict, the Council relies on internationally recognised conventions and authoritative interpretations thereof. Of particular importance is the shared Article 3 of the Geneva Conventions, which protects civilians in non-international armed conflict. Human rights apply irrespective of whether there is a conflict situation. Especially relevant provisions are Articles 6, 7, 9, 17 and 19 of the International Covenant on Civil and Political Rights, which protect the right to life, liberty and security, freedom from torture and freedom of thought and expression.⁷

When assessing a company's contribution to the abuse of such rights, the Council considers that there must be a connection between the company's operations and the abuses concerned. Furthermore, the company must have either contributed actively to the norm violations or known about them without attempting to prevent them in an effective manner. If it is not possible to prevent the norm violations, the Council considers that the company must cease operating in the area. The Official Norwegian Report NOU 2020:7 Values and Responsibility, on the GPF's ethical framework, states that the ethical guidelines are "intended to cover contribution to serious abuses

⁴ See, for example, Report of the Working Group on the issue of human rights and transnational corporations and other business enterprises, Business, human rights and conflict-affected regions: towards heightened action, <https://undocs.org/en/A/75/212>; and Global Compact/PRI's Guidance on Responsible Business in Conflict Affected and High-Risk Areas: A Resource for Companies and Investors, [https://d306pr3pise04h.cloudfront.net/docs/issues_doc%2FPeace and Business%2FGuidance_RB.pdf](https://d306pr3pise04h.cloudfront.net/docs/issues_doc%2FPeace%2FGuidance_RB.pdf).

⁵ Meld. St. 24 (2020–2021) Report to the Storting (white paper) – The Government Pension Fund 2021, <https://www.regjeringen.no/en/dokumenter/meld.-st.-24-20202021/id2843255/>

⁶ See the Council on Ethics' recommendations relating to Kirin Holdings and Adani Ports & Special Economic Zone Ltd, <https://etikkradet.no/tilradninger/alvorlige-krenkelser-av-individers-rettigheter-i-krig-og-konflikt/>

⁷ International Covenant on Civil and Political Rights (ICCPR) with optional protocols, <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights>.

perpetrated by parties other than the company. Companies may be said to contribute to abuses through, for example, supplying goods and services to or entering into business relations with parties to a conflict who perpetrate serious abuses.”⁸

The GPF’s ethical guidelines are forward-looking, and the norm violations must therefore be ongoing or there must be an unacceptable risk that abuses may take place in the future.

When assessing the risk of new abuses, previous norm violations may give an indication of future patterns of behaviour.

1.2 Sources

This recommendation is based on publicly available information from UN bodies, international courts of law, the media, civil society and public bodies, as well as information provided by Sumitomo.

2 Background

2.1 The situation in Myanmar

On 1 February 2021, the armed forces in Myanmar staged a military coup. Hundreds of thousands of civilians protested against the coup through a series of boycotts, strikes and demonstrations across the country. The protesters were met with a violent response by the armed forces and thousands of people have been killed since the generals seized power. Since the coup, the armed conflicts within the country have intensified.⁹ For many years prior to the coup, the armed forces in Myanmar had perpetrated gross abuses against the civilian population. Reported abuses include violence against and the murder of children and adults, gang rape, torture and the torching of whole villages.¹⁰ Many of the victims belong to the Rohingya ethnic minority. On the basis of these abuses, legal proceedings have been initiated in the International Court of Justice (ICJ) for violation of the Convention on the Prevention and Punishment

⁸ NOU 2020: 7 Values and Responsibility – The Ethical Framework for the Norwegian Government Pension Fund Global, chapter 13.3. For the full report in Norwegian, see: <https://www.regjeringen.no/no/dokumenter/nou-2020-7/id2706536/> for a summary in English, see <https://www.regjeringen.no/en/dokumenter/nou-2020-7/id2706536/>.

⁹ United Nations High Commissioner for Human Rights, *Myanmar: UN report calls for urgent action to end human rights catastrophe*, 23 September 2021, <https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=27521&LangID=E>

¹⁰ United Nations Human Rights Council, Report of the independent international fact-finding mission on Myanmar, 12 September 2018, <https://undocs.org/en/A/HRC/39/64>.

of the Crime of Genocide¹¹ and in the International Criminal Court for crimes against humanity.¹²

In a report from March 2023, the UN's Special Rapporteur for Human Rights in Myanmar summed up the situation in the country as follows:

“Two years after Myanmar’s military launched an unconstitutional coup d’état [...] the military has doubled down on its brutal tactics, sowing violence and chaos across an ever-widening sphere of conflict. In recent months, the military has stepped up aerial attacks, bombing villages, schools, medical facilities, and encampments for internally displaced persons. [...] The SAC’s campaign of mass arson continues, with roughly 58,000 homes and civilian structures burned since the coup. More than 1.3 million people have been displaced in the past two years, and more than 3,000 civilians have been killed.

The SAC [State Administration Council] continues to suppress all forms of dissent as it attempts to impose a military-dominated future on the people of Myanmar. More than 16,000 political prisoners are now behind bars. [...] Civilians continue to suffer extrajudicial killings, torture, sexual violence, and other human rights violations, many of which amount to crimes against humanity and war crimes.”¹³

As part of its persecution of political opponents, journalists and activists, the armed forces have increasingly deployed digital weapons such as surveillance drones and software enabling it to hack into PCs, telephones and other electronic devices.¹⁴ It has also been reported that the armed forces have installed an extensive CCTV surveillance system equipped with facial recognition software in several of Myanmar’s major cities. This would increase their capacity to identify political opponents and other persons of

¹¹ International Court of Justice, *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (The Gambia v. Myanmar)*, <https://www.icj-cij.org/en/case/178>

¹² International Criminal Court, *Bangladesh/Myanmar, Situation in the People’s Republic of Bangladesh/Republic of the Union of Myanmar*, <https://www.icc-cpi.int/bangladesh-myanmar>

¹³ UN High Commissioner for Human Rights, Report of the Special Rapporteur on the situation of human rights in Myanmar, Thomas H. Andrews, 9 March 2023, A/HRC/52/66, <https://www.ohchr.org/en/documents/country-reports/ahrc5266-situation-human-rights-myanmar-report-special-rapporteur>

¹⁴ Beech, Hannah, Myanmar’s Military Deploys Digital Arsenal of Repression in Crackdown, The New York Times, 12 March 2021, <https://www.nytimes.com/2021/03/01/world/asia/myanmar-coup-military-surveillance.html>

interest to the authorities.¹⁵ There is no legal basis for the use of video surveillance in Myanmar.

Even before the coup, the Myanmar authorities had initiated a process to gain access to customer data held by mobile phone operators and internet service providers.¹⁶

According to the US State Department, the military had “built an ‘electronic warfare capability’ and bought surveillance technology, including cell phone-hacking tools to monitor prodemocracy activists.”¹⁷

After the coup, the military junta imposed a nationwide block on the internet, social media and messaging platforms. Targeted internet shutdowns have subsequently been implemented in areas where opposition groups are strong. These have coincided with military assaults, the use of violence and arson attacks. According to a press release issued jointly by four of the UN’s Special Rapporteurs, “The imposition of internet shutdowns and throttling on many townships in Sagaing Region in early March” 2022 coincided “with the launch of a major military offensive and campaign of violence and arson against the civilian population in the area.”¹⁸

The regime has also restricted opportunities for anonymous communication by demanding that all users must upload their national ID card or passport to register a SIM card.¹⁹

¹⁵ Potkin, Fanny, Exclusive: Myanmar’s junta rolls out Chinese camera surveillance systems in more cities, Reuters 11 July 2022, <https://www.reuters.com/world/asia-pacific/exclusive-myanmars-junta-rolls-out-chinese-camera-surveillance-systems-more-2022-07-10/>, and Human Rights Watch, Myanmar: Facial Recognition System Threatens Rights, 12 March 2021, <https://www.hrw.org/news/2021/03/12/myanmar-facial-recognition-system-threatens-rights>

¹⁶ Crisis Group, Myanmar’s Military Struggles to Control the Virtual Battlefield, 18 May 2021, Report No 314/ Asia, <https://www.crisisgroup.org/asia/south-east-asia/myanmar/314-myanmars-military-struggles-control-virtual-battlefield>

¹⁷ Beech, Hannah, Myanmar’s Military Deploys Digital Arsenal of Repression in Crackdown, The New York Times 1 March 2021, <https://www.nytimes.com/2021/03/01/world/asia/myanmar-coup-military-surveillance.html> and US Department of State, 2021 Country Reports on Human Rights Practices: Burma, <https://www.state.gov/reports/2021-country-reports-on-human-rights-practices/burma/>

¹⁸ UN High Commissioner for Human Rights in Myanmar: UN experts condemn military’s “digital dictatorship”, Press release 7 June 2022, <https://www.ohchr.org/en/press-releases/2022/06/myanmar-un-experts-condemn-militarys-digital-dictatorship>

¹⁹ Crisis Group, Myanmar’s Military Struggles to Control the Virtual Battlefield, 18 May 2021, Report No 314/ Asia.

Control over the suppliers of mobile phone services enables the authorities to monitor and censor internet traffic and communications, and track the population's use of such services. In this way, the military is able to secure access to user data belonging to opposition figures, members of resistance groups and journalists in order to suppress opponents of the regime. This means that it may be dangerous for people to communicate with each other or visit the websites of independent news sources. In its joint statement, the UN Special Rapporteurs underline that "Online access to information is a matter of life and death for many people in Myanmar, including those seeking safety from indiscriminate attacks by the military and the millions trying to navigate a devastating economic and humanitarian crisis. The junta is using internet shutdowns and invasive surveillance to undermine widespread public opposition and prop up its attacks on the people of Myanmar."²⁰

Two weeks after the coup, the junta presented a draft Cyber Security Law which would, among other things, give the armed forces even greater control of Myanmar's internet and network infrastructure, simplify the shutdown of the internet and give them access to private data.²¹ The proposal was met with fierce opposition from the business community and civil society, and was not adopted.²² Instead, the changes were introduced through amendments to the Electronic Transactions Law, which expanded the authorities' access to personal data and introduced a new ban on online expressions of opinion. An updated draft of the Cyber Security Law was circulated for comment by the business community and telecoms companies in January 2022. This contained no material changes from the previous draft, although it did contain proposals to criminalise private use of virtual private networks (VPN). This would affect millions of people who use VPN to access Facebook and other media sites which are blocked by the armed forces and which are important for information and communication in Myanmar.²³

²⁰ See footnote 18.

²¹ Free Expression Myanmar, Six risks from Myanmar's draft Cyber Security Law, 14 February 2021, <https://freeexpressionmyanmar.org/six-risks-from-myanmars-draft-cyber-security-law/>

²² See footnote 19.

²³ Myanmar Centre for Responsible Business, The Right to Privacy in the Digital Age: Experience from Myanmar, 4 June 2022 <https://www.ohchr.org/sites/default/files/documents/issues/digitalage/reportprivindigage2022/submissions/2022-09-06/CFI-RTP-Myanmar-Centre-Responsible-Business.pdf>, and

In its joint statement, the UN Special Rapporteurs have condemned the military junta's attempts to establish a "digital dictatorship". They confirm that the telecoms companies have been put under severe pressure to activate surveillance technology and hand data over to the police and armed forces. The most recent bill has so far not been passed into law.²⁴

On 1 March 2023, the government in Myanmar amended the anti-terrorism legislation to grant wide-ranging powers to use digital information in the investigation of opponents of the regime, who may now be designated terrorists.²⁵ Chapter 14 of the law includes provisions relating to the tapping, shut-down and restriction of electronic communication, as well as the use of electronic information to verify localisation. A counter-terrorism committee will consider applications from investigative entities (police, military, intelligence) for permission to tap and restrict suspected terrorists' electronic communications. If permission is granted, the telecom operator (licence holder) cannot refuse to shut down, restrict or tap electronic communications. Failure to comply may be punished by fines or terms of imprisonment. Pro-democracy activists believe that the regime will use the law to investigate political opponents by defining them as terrorists.²⁶

2.2 Myanma Posts and Telecommunications (MPT)

MPT is a state-owned company under the authority of the Ministry of Transport and Communications. MPT describes itself as Myanmar's leading telecoms company, which operates a nationwide network infrastructure. The company has many retail outlets and provides the entire country with access to telecommunications services. It has a 96 per cent mobile coverage rate in Myanmar. With regard to its collaboration with Sumitomo

Simpson, Adam, 2022, A Digital Coup Under Military Rule in Myanmar: New Online Avenues for Repression, *Kyoto Review of Southeast Asia Issue 33*, <https://kyotoreview.org/issue-33/a-digital-coup-under-military-rule-in-myanmar/>

²⁴ UN High Commissioner for Human Rights in Myanmar: UN experts condemn military's "digital dictatorship", Press release 7 June 2022, <https://www.ohchr.org/en/press-releases/2022/06/myanmar-un-experts-condemn-militarys-digital-dictatorship>

²⁵ Government of the Republic of the Union of Myanmar Ministry of Home Affairs (Counter-Terrorism Rules) Notification No. (239/2023) 1384, 11th Waxing Day of Tabaung (1 March 2023). Lincoln Legal Services (Myanmar) Limited, Convenience translation – accuracy not guaranteed, <https://www.lincolnmyanmar.com/wp-content/uploads/2023/03/Counter-Terrorism-Rules-abbreviated.pdf>

²⁶ Radio Free Asia, 15.3.2023, Amendment grants Myanmar junta sweeping new powers under Anti-Terrorism Law, <https://www.rfa.org/english/news/myanmar/amendment-03152023170207.html>

and KDDI, MPT's website says: "Together with its workforce of over 8,000 employees and KDDI Summit Global Myanmar (KSGM) all of whom are intensively supporting MPT's operation, MPT is committed to continually driving the development of the telecommunications sector, and moving Myanmar forward."²⁷

MPT is a telecom operator and is licensed to provide telecoms services. MPT describes the agreement with KDDI and Sumitomo as a partnership whose purpose is "to join forces" to make mobile telecoms services available to the country's inhabitants, expand mobile coverage and improve network quality.²⁸ According to MPT, Sumitomo and KDDI provide it with expertise and technology. Since the coup, MPT has been subject to military control.

MPT has made public its Privacy Policy in which the company declares what personal information it collects, how it is used and stored, and how and with whom it is shared. MPT states that it may share information with government agencies "when obligated or ordered to do so under law, warrant, court order, or any other legal or regulatory instruction», but when doing so, it will require that the third party implements "appropriate measures to protect the personal information that they receive, and only process such information in accordance with our instructions."²⁹

3 Sumitomo's business partnership with MPT

Sumitomo and KDDI Corp are partners in a joint venture, KDDI Summit Global Myanmar Co, Ltd (KSGM). KSGM has a Joint Operation Agreement with MPT, which is one of four telecom operators in Myanmar. The joint venture KSGM has built up a telecoms infrastructure and operates mobile network and broadband services in Myanmar in partnership with MPT.

The Joint Operation Agreement with MPT was announced in July 2014. Its purpose was

"to implement, upgrade and expand the national telecommunications service (including mobile, fixed, internet, etc.). KDDI will leverage the experience and technical capabilities it has cultivated as a mobile telecommunications operator in Japan and overseas, and Sumitomo Corporation aims to take advantage of expertise gained through trading with Myanmar and as a mobile telecommunications operator overseas. Together, the two companies intend to contribute to Myanmar's

²⁷ MPT Who we are, <https://mpt.com.mm/en/about-home/>

²⁸ MPT Joint operations, <https://www.mpt.com.mm/en/about-home-en/joint-operation/>

²⁹ MPT Privacy Policy, <https://mpt.com.mm/en/about-home/privacy-policy/>

development in the field of information and telecommunication technology (ICT) and expand their global business.”³⁰

The agreement was further described in Sumitomo’s application for an investment guarantee from the World Bank through the Multilateral Investment Guarantee Agency (MIGA) as follows:

“The JO [joint operation] has approximately 2,000 operational telecommunications towers as of June 2015, some of which will be upgraded or decommissioned and replaced, and plans to construct a further approximately 5,000 towers to meet a target of providing coverage to 70% of the geographical area of Myanmar by the end of March 2016”³¹ Furthermore: “KDDI has the technical expertise required, and SC [Sumitomo Corp] has experience in rolling out telecommunications networks in developing countries. As part of the JOA, KSGM has committed to provide an extensive training program for MPT staff.”³²

Sumitomo provides expertise and advice relating to sales and marketing and the expansion of the network.

4 Surveillance and control of MPT’s customers

In the spring of 2021, several media outlets reported that in the months before the military coup on 1 February Myanmar’s telecom operators had been ordered to install spyware and surveillance software on their systems, which enabled the regime to monitor customers’ telephone and internet usage. The order came from the Ministry of Transport and Communications and applied initially to the Myanmar operators MPT and Mytel.³³ The surveillance, carried out by a dedicated cybersecurity team within the Police

³⁰ Sumitomo and KDDI, Notice of Establishment of Joint Venture in Singapore via Third-Party Capital Allocation, 16 July 2014, https://www.sumitomocorp.com/-/media/Files/hq/news/release/2014/20140716_2/27937_ext_31_0.pdf?la=en og <http://news.kddi.com/kddi/corporate/english/ir-news/2014/07/16/484.html>

³¹ MIGA 2016, Environmental and Social Review. KSGNM Telecommunication Project, [Microsoft Word - Myanmar KSGM ESRS Final Feb 24 2016 FOR DISCLOSURE.docx \(rightsindevelopment.org\)](#)

³² KDDI Corp, KDDI’s mission in Myanmar, Reliable, Japan-quality communication services for Myanmar, <https://www.kddi.com/english/corporate/sustainability/feature1-02/>

³³ Potkin, Fanny and Mcpherson, Poppy, How Myanmar’s military moved in on the telecoms sector to spy on citizens, 19.mai 2021, Reuters, <https://www.reuters.com/world/asia-pacific/how-myanmars-military-moved-telecoms-sector-spy-citizens-2021-05-18/> og Beech,

Special Branch, is supposed to have commenced around a month after the coup. The technology makes it possible to monitor customers in real time and enables the military to tap conversations, read text messages, monitor internet traffic and emails, and track the user's location.

According to an article in the journal *Frontier*, a senior official at MPT told the reporter that "the company [MPT] was not only providing user data to the cybersecurity team but had also dramatically stepped up surveillance of its users since the coup." The official further disclosed: "Two months ago, we [MPT] formed a team to monitor calls. If the system notices a suspicious conversation or detects certain words, the team will be notified. I'm not sure if the recorded conversations are given to the authorities ... but it's no longer safe to speak on the phone."³⁴ The senior MPT official also spoke about the surveillance of internet traffic. The authorities are supposed to have asked the company for information about individuals' internet usage, with arrests being made after the data was handed over.

It has been reported that foreign companies supplied surveillance technology and services enabling the monitoring of telephone conversations before the coup and that such equipment is still in use.³⁵ In January 2023, it became known that Cognyte Software Limited (Cognyte) won a contract in 2020 to supply so-called "lawful interception equipment" to MPT,³⁶ and that the delivery was scheduled for completion in June at

Hannah, Myanmar's Military Deploys Digital Arsenal of Repression in Crackdown, *The New York Times*, 12 March 2021, and *Frontier Myanmar*, Junta steps up phone, internet surveillance – with help from MPT and Mytel, 5. Juli 2021, <https://www.frontiermyanmar.net/en/junta-steps-up-phone-internet-surveillance-with-help-from-mpt-and-mytel/>

³⁴ *Frontier Myanmar*, Junta steps up phone, internet surveillance – with help from MPT and Mytel, 5 July 2021.

³⁵ Mc Dermott, Gerard, Myanmar Is the Leading Edge of Digital Authoritarianism in Southeast Asia, 21 October 2022, *The Diplomat*, <https://thediplomat.com/2022/10/myanmar-is-the-leading-edge-of-digital-authoritarianism-in-southeast-asia/>, and Beech, Hannah, Myanmar's Military Deploys Digital Arsenal of Repression in Crackdown, *The New York Times*, 12 March 2021.

³⁶ Yaron, Oded, Myanmar Acquired Spyware From Israeli Cyber-intelligence Firm Cognyte, *New Docs Reveal - National Security & Cyber*, 15. Januar 2023, *Haaretz*, <https://www.haaretz.com/israel-news/security-aviation/2023-01-15/ty-article/israel-myanmar-acquired-spyware-from-cognyte-new-docs-reveal/00000185-b415-d2c1-afe7-fc37abf40000>.

2021.³⁷ Whether or not the technology was actually delivered or is now in use has not been established. According to Reuters, sources are said to have confirmed that the Cognyte technology was tested by MPT.³⁸

5 Information from the company

The Council on Ethics contacted Sumitomo in July 2022, requesting information about how the coup has affected the company's operations in Myanmar and what measures the company has put in place to avoid contributing to human rights violations.

Sumitomo responded in August 2022, since when the Council has communicated with the company on several occasions, most recently in June 2023.

In September 2021, Sumitomo wrote on its website: "We are deeply concerned about the situation in Myanmar regarding lawful interception and mobile internet shutdown in light of the importance of ensuring the use of communication for everyone and protecting its privacy from the perspective of human rights." The company said that it is not "subject to direct instructions from the regulatory authority with regard to interception based on the telecommunications laws of Myanmar." Furthermore, it has asked MPT "to ensure that proper process is secured for each individual case so that the basic human rights of the people of Myanmar are not negatively affected and that tangible and intangible assets provided by KSGM are not used in situations that violate the Sumitomo Corporation Group's Human Rights Policy".³⁹

According to Sumitomo, the authorities in Myanmar ordered all telecom operators to shut down the mobile network after the coup, but that restrictions have gradually been lifted. Nevertheless, restrictions still apply in some areas. The company has notified the Council that it performs regular due diligence assessments to identify potential human

³⁷ Justice For Myanmar, Israeli surveillance firm Cognyte's business in Myanmar exposed, 15 January 2023, <https://www.justiceformyanmar.org/stories/israeli-surveillance-firm-cognytes-business-in-myanmar-exposed>

³⁸ Potkin, Fanny & McPherson, Poppy, Israel's Cognyte won tender to sell intercept spyware to Myanmar before coup – documents, Reuters, 18 January 2023, <https://www.reuters.com/technology/israels-cognyte-won-tender-sell-intercept-spyware-myanmar-before-coup-documents-2023-01-15/>. In June 2022, the Council recommended that Cognyte be excluded from investment by the Norwegian GPF because the company's products and services could have enabled serious norm violations in South Sudan, Azerbaijan, Indonesia and Bahrain, among others.

³⁹ Sumitomo Corp, Sumitomo Corporation's Stance on Telecommunications Business in Myanmar, 29 September 2021, <https://www.sumitomocorp.com/en/jp/news/important/group/20210929>

rights violations relating to the project. “Violation of the right to privacy by interception” is one of the risks that have been identified.

With regard to its relationship with MPT, Sumitomo wrote that it has been “supporting MPT’s operations” and that the company’s employees contribute with know how, advice on sales and marketing and network expansion. The company has made it clear to the Council that it plays no role in any monitoring of MPT’s customers and that it is MPT, as licence holder, that is subject to the authorities’ orders. As employees of the state, MPT’s staff are not permitted to give any information about the authorities’ orders to the company’s business partners.⁴⁰

Sumitomo called on “MPT to ensure that proper process is secured for each individual case [internet shutdowns] so that the basic human rights of the people of Myanmar are not negatively affected. Aiming for a full and immediate lifting of the mobile internet shutdown, we have been making efforts to fully restore the internet in collaboration with other telecommunications service providers by, for example, issuing a written request to the regulatory authority.” At the same time, the company believes it is not “in a position to explain the detail of MPT’s operation and how MPT reacted with our requests to improve from the human rights perspective. However, we think that MPT has been taking our request seriously. We will continue to request MPT to take appropriate measure in order to respect the basic human rights of the people of Myanmar.”⁴¹

In its letter to the Council, Sumitomo wrote that it was extremely concerned about the human rights situation in Myanmar, which it considers has impacted the company’s operations. Nevertheless, the company feels that it is important to remain in the country because “our technical and sales support activities are indispensable for maintaining the communication services that are the lifeline of the people of Myanmar. At present, we believe that continuing our business and continuing our approach to the regulated authorities and MPT will assist with the better fulfilment of human rights of the people of Myanmar.”⁴² The company further declared that “Exit from the Project would, however, risk significant adverse impacts on rightsholders, above all our customers. Access to mobile and fiber internet connectivity is an ‘essential service’ which supports their enjoyment of a number of human rights such as health, education, livelihoods, and information,” and added “We predict that our exit would result in adverse impacts on

⁴⁰ Letter from Sumitomo to the Council on Ethics, dated 18 August 2022.

⁴¹ Letter from Sumitomo to the Council on Ethics, dated 18 August 2022.

⁴² Letter from Sumitomo to the Council on Ethics, dated 18 August 2022.

human rights, due to reduced internet access which, were we to depart, we would be unable to mitigate.”⁴³

6 The Council’s assessment

The Council on Ethics has assessed the GPF’s investment in Sumitomo against the ethical guidelines’ criterion relating to serious violation of the rights of individuals in situations of war or conflict. In its assessment of the company’s contribution to such violations, the Council takes the position that companies must exercise particular care when they operate in areas where war or conflict is ongoing.

The extremely serious abuses perpetrated against the civilian population in Myanmar are well documented and constitute serious violations of humanitarian law and human rights. Since the coup, many civilians have been killed and even more imprisoned. Uprisings and armed resistance against the coup have been met with intensified use of force and abuse, in terms of both scale and seriousness. The Council considers that the risk of the military continuing to commit new, extremely serious abuses is high. Due to the risk of contributing to these serious abuses, companies operating in Myanmar must exercise particular care.

Based on the information available concerning surveillance of the telecoms network in Myanmar, the Council presumes that MPT, which is subject to the authority of the government in Myanmar, has installed technology which enables the surveillance of civilians, that the surveillance has been ramped up after the coup, and that police and military units have access to the surveillance data generated by MPT. It is not known how the data from MPT has been used by the police and armed forces. However, it is known that surveillance has enabled extremely serious norm violations. This includes the arrest of opponents of the regime on the basis of the information obtained through surveillance. MPT’s handover of personal data entails a considerable risk of targeting the civilian populations and that individuals’ right to liberty and safety, the right to freedom from torture, the right to a private life and the right to freedom of expression will be infringed. While the amendments to the anti-terror legislation have introduced a formalised structure, it is the assessment of the Council that the amendments largely seem to have been designed to facilitate intensified persecution of political opponents and thereby also the risk of serious norm violations.

Sumitomo is a partner in a joint venture that has a Joint Operation Agreement with MPT. For many years, it has helped to build up MPT’s capacity and competence with regard to telecoms services. The agreement means the companies jointly operate the telecoms

⁴³ Letter from Sumitomo to the Council on Ethics dated 12 June 2023.

business, with MPT as the licence holder and operator. When assessing Sumitomo's contribution to norm violations, the Council attaches importance to the fact that the company is engaged in a business association with a partner that enables serious and systematic violations of human rights and humanitarian law. Although Sumitomo plays no direct role in the surveillance, the Council assumes that Sumitomo must know that MPT has installed and activated tools which enable the regime to monitor human rights activists, political opponents and other individuals.

In its dialogue with the Council, Sumitomo said that it performs due diligence assessments in order to identify and mitigate negative human rights impacts related to its operations, that it has attempted to use its influence to address the risk of human rights abuses relating to surveillance, and that it has called on MPT to take account of human rights. Although this is positive, the Council considers that the steps the company has taken to prevent its contribution to human rights violations have produced very few tangible results.

The Council notes that the company continuously assesses the human rights situation in the country, and that it has so far, elected to remain in Myanmar out of consideration for its own employees and to help maintain the telecoms infrastructure that is also vital for the civilian population. The Council acknowledges that the choice between remaining in the country and pulling out represents a potential dilemma for the company and that it has limited freedom of action in its partnership with MPT.

Nevertheless, the Council considers that this cannot be accorded decisive weight when there is a considerable risk that MPT will continue to hand customer data over to the authorities, which will enable serious abuses to be perpetrated against the civilian population. While the military holds power in the land, it is unlikely that Sumitomo will wield sufficient influence to prevent this. The Council concludes, therefore, that as long as Sumitomo's partnership with MPT persists, the risk of the company contributing to the violation of the rights of individuals in situations of war or conflict will remain at an unacceptable level.

7 Recommendation

The Council on Ethics recommends that Sumitomo Corp be excluded from investment by the Government Pension Fund Global (GPF) pursuant to the ethical guidelines' criterion on the serious violation of the rights of individuals in situations of war or conflict.

Svein Richard
Brandtzæg
Leder

(Sign.)

Siv Helen Rygh
Torstensen

(Sign.)

Cecilie
Hellestveit

(Sign.)

Vigdis
Vandvik

(Sign.)

Egil Matsen

(Sign.)