

Unofficial English translation

**To Norges Bank**

17.06.2022

**Recommendation to exclude Cognyte Software Ltd from investment by the Norwegian Government Pension Fund Global (GPF)**

## Summary

The Council on Ethics recommends that Cognyte Software Ltd (Cognyte) be excluded from investment by the Norwegian Government Pension Fund Global (GPFG) due to an unacceptable risk that the company is contributing to serious human rights abuses. The recommendation relates to human rights abuses that may be enabled by the company's products and services.

Cognyte is an Israeli company that supplies surveillance software. Cognyte was previously part of Verint Systems (Verint), but was spun off as an independent company in 2021. Cognyte is listed on the Nasdaq exchange in the USA. At the close of 2021, the GPFG owned 0.87 per cent of the company's shares, worth NOK 79 million.

Based on publicly available information, the Council considers that Cognyte's products and services may have enabled serious norm violations. The company provides bespoke technological solutions, as well as training, service and maintenance. Several of the states that are said to be among its customers have been accused of extremely serious human rights violations, including abduction, torture and other forms of abuse targeting vulnerable groups, including sexual minorities. The accusations are wide-ranging and relate to many different countries.

An important factor for the Council is that the company must have known that some of its customers have been accused of extremely serious human rights violations. The Council also considers that surveillance of political opponents and minorities is a foreseeable risk for the company, given the products and services it offers.

With regard to the risk going forward, the Council attaches importance to the emergence, as recently as December 2021, of information that Cognyte's solutions had been used for the surveillance of politicians and journalists. The Council considers that the information which Cognyte has shared with it does not adequately address the serious allegations made against the company. The Council has been particularly keen to understand what measures the company has implemented to avoid involvement in such norm violations in the future, but has received only superficial answers from the company. The Council therefore concludes that there is an unacceptable risk of Cognyte contributing to human rights violations.

# Contents

|          |   |          |
|----------|---|----------|
| <b>1</b> | <b>Introduction</b>   | <b>1</b> |
| 1.1      | Matters considered by the Council                             | 1        |
| 1.2      | Human rights and surveillance technology                      | 2        |
| 1.3      | Sources   | 3        |
| <b>2</b> | <b>About the company</b>                                      | <b>3</b> |
| <b>3</b> | <b>Accusations of contributing to human rights violations</b> | <b>4</b> |
| <b>4</b> | <b>Information provided by the company</b>                    | <b>6</b> |
| <b>5</b> | <b>The Council's assessment</b>                               | <b>7</b> |

# 1 Introduction

The Council on Ethics for the Norwegian Government Pension Fund Global (GPF) has assessed the fund's investment in Cognyte Software Ltd<sup>1</sup> (Cognyte) against the Guidelines for Observation and Exclusion of Companies from the Government Pension Fund Global (the ethical guidelines).<sup>2</sup> This recommendation relates to human rights abuses that may have been enabled by the company's products and services.

Cognyte is an Israeli software company that supplies surveillance products and services. Cognyte was previously part of Verint Systems (Verint), but was spun off as a separate company in 2021.<sup>3</sup> Cognyte is listed on the Nasdaq exchange in the USA.

At the close of 2021, the GPF owned 0.87 per cent of the company's shares, worth NOK 79 million.

## 1.1 What the Council has considered

The Council on Ethics has assessed the GPF's investment in Cognyte against section 4(a) of the ethical guidelines: "Companies may be excluded or placed under observation if there is an unacceptable risk that the company contributes to or is responsible for [...] serious or systematic human rights violations."

When assessing whether a company has contributed to serious or systematic human rights violations, the Council relies on internationally recognised conventions and authoritative interpretations thereof. This recommendation rests primarily on the right to freedom and safety, freedom from torture and the right to privacy, as protected by the Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment (the Torture Convention) and the International Covenant on Civil and Political Rights. Both conventions prohibit discrimination on the grounds of ethnicity, religion or sexual orientation.<sup>4</sup> The Council also attaches importance to the UN Guiding Principles on Business and Human Rights.<sup>5</sup> When assessing the seriousness of norm violations, the Council attaches importance to the scope and consequences of the infringements, and the extent to which it is possible to mitigate those consequences. The Council also attaches importance to whether the norm violations impact particularly vulnerable groups.

Although international human rights conventions bind states not companies, companies can be said to contribute to human rights abuses. The Council takes no position on whether states are responsible for any human rights violations. It is sufficient to conclude that the company concerned is behaving in such a way as to contribute to serious or systematic violations of internationally recognised human rights.

When assessing whether a company can be said to contribute to human rights abuses, the Council considers that there must be a link between the company's operations and the norm

---

<sup>1</sup> Issuer ID: 66664579

<sup>2</sup> Guidelines for Observation and Exclusion of Companies from the Government Pension Fund Global (GPF), <https://files.nettsteder.regjeringen.no/wpuploads01/sites/275/2021/11/Guidelines-for-Observation-and-Exclusion-GPF-29-November-2021.pdf>

<sup>3</sup> Cognyte, *Our Story*, <https://www.cognyte.com/about/>

<sup>4</sup> UN Human Rights Council, *Discriminatory laws and practices and acts of violence against individuals based on their sexual orientation and gender identity*, 2011 [https://www.ohchr.org/documents/issues/discrimination/a.hrc.19.41\\_english.pdf](https://www.ohchr.org/documents/issues/discrimination/a.hrc.19.41_english.pdf)

<sup>5</sup> UN High Commissioner for Human Rights, *UN Guiding Principles on Business and Human Rights*, 2011 [https://www.ohchr.org/documents/publications/GuidingprinciplesBusinesshr\\_eN.pdf](https://www.ohchr.org/documents/publications/GuidingprinciplesBusinesshr_eN.pdf)

violations in question, and the company must have actively contributed to the violation or known about it without doing anything to prevent it. In a previous recommendation, the Council concluded that the development and sale of surveillance equipment had enabled serious human rights violations.<sup>6</sup>

Norm violations must be ongoing or there must be an unacceptable risk that abuses may occur in future. When assessing the risk of new abuses, previous norm violations may give an indication of future patterns of behaviour. The Council attaches importance to what the company is doing to prevent norm violations, particularly the company's overarching human rights policy and how this is implemented in practice, e.g. through due diligence inquiries, governance systems and guidance at the operational level.

## 1.2 Human rights and surveillance technology

In August 2021, a group of UN experts asked the UN member states to introduce a *global moratorium* on the sale and transfer of surveillance technology. The experts felt it was necessary to halt such sales until a robust regulatory framework had been put in place to ensure the technology was used in compliance with human rights.<sup>7</sup> The experts were extremely concerned that sophisticated and intrusive tools were being used to surveil, intimidate and silence human rights defenders, journalists and political opponents. The experts considered such behaviour violated the right to liberty, privacy and freedom of expression, and that the technology could put hundreds of lives at risk. The experts referred to a 2019 report from the UN Special Rapporteur on Freedom of Opinion and Expression, which also advocates a halt to sales of surveillance technology. In their report, the Special Rapporteur also discusses the role of companies in this matter:

*Because the companies in the private surveillance industry operate under a cloak of secrecy, the public lacks any information about the way in which they may – if at all – consider the human rights impacts of their products. Given the nature of the industry and the widespread use of its products for purposes that are inconsistent with international human rights law, it is difficult to imagine that they do in fact take such impacts into account. Put another way: given the broad public knowledge of the repression practised by many of their clients, the companies cannot seriously claim to lack insight into the repressive uses of their tools.<sup>8</sup>*

The Special Rapporteur recommended that companies in this sector both perform thorough due diligence investigations to avoid contributing to human rights violations and implement robust measures to prevent misuse of their products and services. The same expectations with respect to companies are set out in the publication “*Navigating the surveillance technology ecosystem: A human rights due diligence guide for investors*” published by the Business and Human Rights Resource Centre et al. The guide illustrates how various types of surveillance equipment can negatively impact different human rights, including the right to liberty and

---

<sup>6</sup> The Council on Ethics, Hangzhou Hikvision Digital Technology Co Ltd, 18 September 2020  
<https://etikkradet.no/hangzhou-hikvision-digital-technology-co-ltd-2/>

<sup>7</sup> UN High Commissioner for Human Rights, *Spyware scandal: UN experts call for moratorium on sale of ‘life threatening’ surveillance tech*, 14 August 2021  
<https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=27379&LangID=E>

<sup>8</sup> UN Human Rights Council, *Surveillance and human rights, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, 28 May 2019,  
<https://undocs.org/A/HRC/41/35>

security of person, freedom from torture and the right to privacy.<sup>9</sup> The guide also points to various risk factors linked to companies. For example, a substantial risk appears to attach to companies whose entire business relates to surveillance technology, which lack a clear human rights policy and which have been linked to multiple human rights abuses without addressing them.

### 1.3 Sources

The Council has made use of publicly available information, including reports and other material from public bodies, the UN, civil society and the media. The Council has also been in contact with the company.

## 2 About the company

Cognyte describes itself as a global leader in “*investigative analytics software*”.<sup>10</sup> The company was established in May 2020 and was spun off as an independent listed company in 2021, having previously been part of Verint. On 1 February 2021, Verint announced that the demerger of its Cyber Intelligence Solutions entity had been completed and would continue in the newly established company, Cognyte.<sup>11</sup> As a result of the demerger, Verint transferred the entire business from the previous entity to the new company, including customers, employees and office facilities. In its annual report, Cognyte writes that the bulk of its revenues come from existing customers.<sup>12</sup> The company has also signed several long-term contracts,<sup>13</sup> which is normal in the security sector.<sup>14</sup>

Cognyte discloses that it has over 1,000 public and private customers, including national security services, in more than 100 countries. The bulk of Cognyte’s revenues derive from services sold to national governments in various countries. The company has around 2,000 employees, mostly based in Israel.

This is how the company describes itself:

*Cognyte is a global leader in investigative analytics software that empowers governments and enterprises with Actionable Intelligence for a Safer World™. Over 1,000 government and enterprise customers rely on Cognyte’s solutions to accelerate and conduct investigations and derive insights, with which they identify, neutralize, and tackle threats. Our open analytics software fuses, analyzes, and visualizes disparate data sets at scale to help organizations find the needles in the haystacks and transform data into insights they can act upon, fast. We empower our customers to*

---

<sup>9</sup> Business and Human Rights Resource Centre et al., *Navigating the surveillance technology ecosystem: A human rights due diligence guide for investors. Annex 1*, mars 2022  
[https://www.accessnow.org/cms/assets/uploads/2022/03/2022\\_STAP\\_Guide.pdf](https://www.accessnow.org/cms/assets/uploads/2022/03/2022_STAP_Guide.pdf)

<sup>10</sup> Cognyte, *About us*, <https://www.cognyte.com/about/>

<sup>11</sup> United States Securities And Exchange Commission, Filing by Cognyte Software Ltd, page 52, 13 January 2021 <https://www.sec.gov/Archives/edgar/data/0001824814/000119312521008526/d52351d20fr12ba.htm>

<sup>12</sup> Cognyte Software Ltd., *Annual Report 2021* filed to US SEC <https://cognyte.gcs-web.com/static-files/798ceabb-7dfa-4492-874b-7d236e86ce37>

<sup>13</sup> Cognyte Software Ltd., *Annual Report 2021* filed to US SEC

<sup>14</sup> There may be several reasons for this, including so-called “technical lock-in”, which means that it is difficult for the user to switch to a different supplier because the software is part of a larger context where multiple products have been tailored to operate in concert. In many cases, the supplier’s employees must have security clearance in order to implement the product, which can be a lengthy and resource-intensive process.

*address a broad range of security challenges, including threats to national security, business continuity, and cyber security.*<sup>15</sup>

The company has further reported that it offers customers “a powerful analytics platform with a rich set of analytics engines, artificial intelligence and machine learning models, workflows, data governance, and visualization tools.” The platform supplied by the company uses customer data and can be integrated with the solutions the customer already uses. The company supplies specially customised software solutions and offers extensive training and support services to customers.

An article in Forbes magazine about the syphoning of information from smart phones describes Verint and Cognyte as follows:

*It sells all manner of spy tools, including one that can locate any individual to the nearest cell tower with just their telephone number. Combining that with advertising data, which provides more specific coordinates of a device’s whereabouts, would likely yield the location of many individuals.*<sup>16</sup>

### **3 Accusations of contribution to human rights violations**

Investigating a company’s contribution to human rights violations in the security sector is impeded by the very fact that the products and services concerned are meant to operate in secret. Nevertheless, some information about the company’s links to human rights violations in several countries has come to light.

#### *Report by Meta*

The company Meta performed an extensive survey of the private surveillance services which use Meta’s platforms to surveil and influence individuals, including Cognyte,<sup>17</sup> and published its results in the report entitled “*Threat Report on the Surveillance-for-Hire Industry*” in December 2021. According to the report:

*While these “cyber mercenaries” often claim that their services only target criminals and terrorists, our months-long investigation concluded that targeting is in fact indiscriminate and includes journalists, dissidents, critics of authoritarian regimes, families of opposition members and human rights activists.*<sup>18</sup>

The report further states that Cognyte has established a series of false profiles on Meta’s platforms “to social-engineer people and collect data”.<sup>19</sup> According to the report, Cognyte had customers in Israel, Serbia, Colombia, Kenya, Morocco, Mexico, Jordan, Thailand and Indonesia. The surveillance targeted journalists and politicians around the world. The report discloses that Meta has deleted around 100 accounts created by Cognyte, that the companies

---

<sup>15</sup> Cognyte, *Our Story*, <https://www.cognyte.com/about/?source=SocialOrg>

<sup>16</sup> Forbes, *Exclusive: Israeli Surveillance Companies Are Siphoning Masses Of Location Data From Smartphone Apps*, 11 December 2020 <https://www.forbes.com/sites/thomasbrewster/2020/12/11/exclusive-israeli-surveillance-companies-are-siphoning-masses-of-location-data-from-smartphone-apps/?sh=4c32ef6438fc>

<sup>17</sup> Meta, *Threat Report on the Surveillance-for-Hire Industry*, December 2021

<https://about.fb.com/wp-content/uploads/2021/12/Threat-Report-on-the-Surveillance-for-Hire-Industry.pdf>

<sup>18</sup> Meta, 2021 p. 2

<sup>19</sup> The Meta report describes the term in this way: “[...] the operators typically rely on social engineering tactics and use fictitious personas to reach out to people via email, phone calls, text messages, or direct messages on social media. [...] The social engineering aims can range from obtaining sensitive information desired by the client to targeting the individual with malware to enable full-device digital surveillance.”

mentioned in the report have been blocked from using the platforms and that several have been given a warning for breach of Meta's terms and conditions of use.

### *South Sudan*

A report published by Amnesty International in February 2021<sup>20</sup> alleged that Verint has supplied bugging devices and support services to the authorities in South Sudan, including the national security services, which have been accused of extremely serious human rights violations, including arbitrary detention, torture and murder.<sup>21</sup>

Verint is said to have provided these services through a telecommunications company that operated in South Sudan up until 2018. Amnesty claimed to have seen documents proving that the telecommunications company paid at least USD 762,236 to Verint in the period 2015–2017 at the behest of the country's authorities. The company did not reply to Amnesty's questions about this matter.

As far back as 2016, Associated Press (AP) named Verint as a possible supplier of surveillance equipment to South Sudan.<sup>22</sup> In October 2018, after speaking with a former company employee, the Israeli newspaper Haaretz reported that Verint was providing services to the country.<sup>23</sup> In 2016, the UN's Panel of Experts on South Sudan stated in a letter that the country's authorities had obtained Israeli surveillance equipment.<sup>24</sup> According to the letter, the security services' ability to "*identify and illegally apprehend individuals has been significantly enhanced since the beginning of the conflict because it has acquired additional communications interception equipment from Israel*".

### *Azerbaijan*

According to the Haaretz article from 2018, Verint is alleged to have sold spyware and intelligence gathering software to Azerbaijan.<sup>25</sup> The newspaper quotes someone who had received training in Verint's products and services in the country, and who said that he had been asked how one could discover "sexual inclinations" via Facebook. The abuse of people on the basis of their sexual orientation or gender expression in Azerbaijan is well documented, not least by Human Rights Watch (HRW).<sup>26</sup> Abuses include arbitrary detention and torture, including the use of electroshock devices. A case relating to such abuse has also been tried in the European Court of Human Rights in Strasbourg.<sup>27</sup>

### *Indonesia*

It has been reported that Verint's products may have enabled human rights violations in Indonesia.<sup>28</sup> A source has disclosed that Verint's systems have been used to create an overview of activists working to promote LGBT rights. Another source told of systematic

---

<sup>20</sup> Amnesty International, South Sudan: "*These walls have ears*": *The chilling effect of surveillance in South Sudan*, 2 February 2021, <https://www.amnesty.org/en/documents/afr65/3577/2021/en/>

<sup>21</sup> See the recommendation relating to Oil & Natural Gas Corp Ltd, <https://etikkradet.no/oil-natural-gas-corp-ltd/>

<sup>22</sup> Associated Press, *Snapping up cheap spy tools, nations 'monitoring everyone'*, 2 August 2016 <https://apnews.com/article/736dd5c3aa644cd499d6f6da8b9e5974>

<sup>23</sup> Haaretz, *Revealed: Israel's Cyber-spy Industry Helps World Dictators Hunt Dissidents and Gays*, 20. oktober 2018 <https://www.haaretz.com/israel-news/.premium.MAGAZINE-israel-s-cyber-spy-industry-aids-dictators-hunt-dissidents-and-gays-1.6573027>

<sup>24</sup> UN Panel of Experts on South Sudan, *Letter to the to the President of the Security Council*, 22 January 2016 <https://digitallibrary.un.org/record/817920>

<sup>25</sup> Haaretz (2018)

<sup>26</sup> Human Rights Watch, *Azerbaijan: Anti-Gay Crackdown*, 3 October 2017 <https://www.hrw.org/news/2017/10/03/azerbaijan-anti-gay-crackdown>

<sup>27</sup> European Court of Human Rights, *A v Azerbaijan (no. 17184/18)*, 26 February 2019 <https://hudoc.echr.coe.int/eng#%7B%22appno%22:%5B%2217184/18%22%5D,%22itemid%22:%5B%22001-192028%22%5D%7D>

<sup>28</sup> Haaretz (2018)



surveillance of religious minorities. The abuse of sexual and religious minorities in Indonesia is well documented by HRW and others.<sup>29</sup>

#### *Bahrain*

It has been reported that Verint has supplied the government in Bahrain with surveillance systems which have been used in part to surveil people via social media.<sup>30</sup> It is known that the country's government has taken extreme measures to suppress critics of the sitting regime.<sup>31</sup> It has also been reported that the government has used surveillance services from another supplier to obtain information about opponents of the regime, who have subsequently been tortured.<sup>32</sup>

#### *Other countries*

It has further emerged that the company's services have been sold to a number of countries in addition to those mentioned above and may have been involved in norm violations there. This includes Uzbekistan, Kazakhstan,<sup>33</sup> Colombia<sup>34</sup> and Peru.<sup>35</sup>

## **4 Information provided by the company**

The Council on Ethics has engaged in written correspondence with the company in the period from July 2021 to June 2022. The company writes that it respects human rights, that the company is one of the most responsible within its sector and that its products and services promote human rights by preventing crime and terrorism. Although the company's solutions have always been sold for lawful and legitimate purposes, the company cannot fully safeguard itself against their misuse. The company is, moreover, clear that it complies with all prevailing laws and regulations, including its own *Code of Conduct* and *Third-Party Code of Conduct*.<sup>36</sup>

Cognyte further writes that the company addresses human rights issues through its internal investigations, guidelines, training, etc. The company has also used its spinoff from Verint to improve its compliance systems and guidelines. The company was unable to comment on specific allegations. Cognyte has stated that it has been in dialogue with Meta regarding Meta's report, and that Meta had not taken "*any actions against Cognyte*". The company made no reply about whether it had received a warning, was banned from the platforms or that accounts had been deleted.

---

<sup>29</sup> See, for example: Human Rights Watch, *Religious Minorities in Indonesia Face Discrimination*, 2020 <https://www.hrw.org/news/2020/12/24/religious-minorities-indonesia-face-discrimination>, *The Human Cost of Indonesia's Blasphemy Law*, 2018 <https://www.hrw.org/news/2018/10/25/human-cost-indonesias-blasphemy-law> and *Human Rights Watch World Report 2021, Indonesia Events of 2020* <https://www.hrw.org/world-report/2021/country-chapters/indonesia>

<sup>30</sup> Haaretz (2018)

<sup>31</sup> Human Rights Watch, *Human Rights Watch World Report 2021, Bahrain Events of 2020* <https://www.hrw.org/world-report/2021/country-chapters/bahrain>

<sup>32</sup> Bloomberg, *Torture in Bahrain Becomes Routine With Help From Nokia Siemens*, 22 August 2011, <https://www.bloomberg.com/news/articles/2011-08-22/torture-in-bahrain-becomes-routine-with-help-from-nokia-siemens-networking>

<sup>33</sup> Privacy International, *Private Interests: Monitoring Central Asia*, 12 November 2014 <https://privacyinternational.org/report/837/private-interests-monitoring-central-asia>

<sup>34</sup> Privacy International, *Press Release: Companies From The UK, The US, And Israel Provided Mass Surveillance Capabilities To Colombian Security Services*, 2 September 2015 <https://privacyinternational.org/press-release/712/press-release-companies-uk-us-and-israel-provided-mass-surveillance-capabilities>

<sup>35</sup> Haaretz (2018)

<sup>36</sup> Cognyte, *Ethics and Code of Conduct*, <https://www.cognyte.com/code-of-conduct/>

In its 2021 annual report, Cognyte discusses human rights issues under the heading: “*Reputational and political factors related to our business or operations may adversely affect us*”.<sup>37</sup> Here, the company comments on the Meta report and says that Meta found that Cognyte had used its platforms in breach of its terms and conditions of use. The company further states that the sale of products and services to countries perceived as having a poor human rights record could lead to negative reports and harm Cognyte’s reputation, even though its operations are legal where they take place. The company further states that some of the products it sells are perceived to be especially powerful and intrusive, and that civil society and others have therefor trained a particularly critical searchlight on the company. Such negative reports could also lead to reputational loss. The company considers that this is a risk that could increase as it expands its business operations.

## **5 The Council’s assessment**

The Council on Ethics has assessed the GPFG’s investment in Cognyte against the human rights criterion in the ethical guidelines.

The question in this case is whether there is an unacceptable risk that the company, through its sales of products and services, could have enabled serious norm violations. Several of the states that are said to be customers of the company have been accused of extremely serious human rights violations, including abduction, torture and other forms of abuse targeting vulnerable groups, including sexual minorities. These accusations are wide-ranging and relate to many different countries.

The Council considers that the accusations relating to Verint are relevant for an assessment of the GPFG’s investment in Cognyte, since Cognyte is a continuation of Verint’s surveillance business. Cognyte itself reports that around 90 per cent of its revenues derive from existing customers. Long-term contracts are also normal in this business sector.

Although the Council has not taken a position on the moratorium proposed by UN experts, it recognises that surveillance technology can enable states to carry out human rights violations. Based on the available information, the Council considers that this may be the case for Cognyte’s products and services. According to the company itself, Cognyte’s solutions are powerful. Publicly available information indicates that the solutions could significantly enhance its customers’ ability to surveil their targets. The company provides specially customised technological solutions, as well as training, service and maintenance. For its part, the company has explained that its products and services promote human rights because they can prevent crime and terrorism. The Council sees no conflict between the products having such a purpose and effect, and being used to enable serious abuses.

The Council notes reports and witness testimony indicating that the company’s products and services have been used to surveil political opponents as well as ethnic and sexual minorities in countries like South Sudan, Azerbaijan, Indonesia and Bahrain. The Council attaches importance to the fact that the company must have known that some of its customers are guilty of extremely serious human rights violations. The Council also considers that the accusations regarding the surveillance of political opponents and vulnerable minorities also constitute a foreseeable risk for the company, given the products it sells. With regard to future risk, the Council attaches importance to the disclosure, as recently as December 2021, that Cognyte’s services have been used to surveil politicians and journalists.

---

<sup>37</sup> Cognyte, *Annual Report 2021 filed to US SEC*

In its dialogue with the Council, the company has referred to its internal guidelines, but these documents contain no information about the risk of human rights violations that this case concerns. The company’s annual report deals with human rights primarily in connection with the risk of harm to its reputation. The Council considers that the information the company has shared does not adequately address the serious allegations that have been made. The Council has been particularly keen to understand how the company intends to avoid being involved in such norm violations going forward, but has received only superficial answers. Based on the available information, it is not possible to determine that the company has initiated appropriate measures to avoid being involved in new norm violations in the future. The Council therefore concludes that there is an unacceptable risk that Cognyte is contributing to serious human rights abuses.

## 6 Recommendation

The Council on Ethics recommends that Cognyte Software Ltd be excluded from the Government Pension Fund Global.

\*\*\*

Johan H.  
Andresen  
Chair  
(Sign.)

Svein Richard  
Brandtzæg  
(Sign.)

Cecilie  
Hellestveit  
(Sign.)

Trude  
Myklebust  
(Sign.)

Siv Helen Rygh  
Torstensen  
(Sign.)