

Satya Nadella  
Chief Executive Officer  
Microsoft Corporation  
One Microsoft Way Redmond,  
WA 98052-6399  
USA

April 11, 2023

RE: Microsoft Corporation's business operations in Russia

Dear Mr. Nadella,

We write to you as [B4Ukraine](#), a coalition of Ukrainian and international civil society organizations working to curtail the financial resources enabling the Russian invasion of Ukraine. In the spirit of respect for the fundamental rights of all people, the rules-based international order, and a prosperous global economy, we expect companies to demonstrate public support for the people, democracy, and territorial integrity of Ukraine, opposition to Russia's war of aggression, and alignment with the UN Guiding Principles on Business and Human Rights (UNGPs).

We request an urgent dialogue regarding potential inconsistencies between Microsoft Corporation's (Microsoft's) obligations under international humanitarian and human rights law and the company's ongoing business operations and relationships in Russia that may contribute to, or be linked with, human rights harms.

It has been over one year since Russia invaded Ukraine and the devastating impacts continue to shock the global conscience and shake the global economy. Russia is violating international humanitarian law (IHL), including war crimes and crimes against humanity, through attacks on civilians and civilian infrastructure (e.g., mass executions, sexual violence, torture, forcible transfer of civilians). More than 22,000 Ukrainians have been killed and injured and millions more have been forced to flee their homes, creating one of the largest humanitarian and refugee crises of modern times. In recognition of the severity of abuses, in March 2023 the International Criminal Court issued an arrest warrant for Vladimir Putin to answer war crimes charges for an alleged scheme to deport Ukrainian children to Russia.<sup>1</sup>

Moreover, as outlined below, recent developments in Russia point to an expanding universe of financial, legal, and reputational risks facing remaining companies.

On September 21, President Vladimir Putin escalated the war by announcing a "partial mobilisation" of the Russian population. The accompanying legislation ([Article 9 of Federal Law No. 31-FZ](#)) mandates all organisations, including the more than 1,500 international companies that are

---

<sup>1</sup> International Criminal Court, "Situation in Ukraine: ICC judges issue arrest warrants against Vladimir Vladimirovich Putin and Maria Alekseyevna Lvova-Belova," March 17, 2023, <https://www.icc-cpi.int/news/situation-ukraine-icc-judges-issue-arrest-warrants-against-vladimir-vladimirovich-putin-and> (accessed March 22, 2023).

currently operating on a full or limited scale in Russia, to conduct military registration of the staff if at least one of the employees is eligible for military service.<sup>2</sup> They must also assist with delivering the military summons to their employees, ensure the delivery of equipment to assembly points or military units, and provide information, buildings, communications, land plots, transport, and other material means of support to the war effort.

A new decree issued by President Putin on March 3, 2023, enables the Russian government to suspend shareholders' rights and implement external management in companies that don't fulfil state defence contracts under conditions of martial law.<sup>3</sup> By specifying the process of appointing Russian government representatives to manage businesses that fail to meet state orders, the latest Decree effectively creates a scenario of "partial nationalization."

With new legislation introducing partial mobilisation, nationalisation, and potentially martial law in Russia, it is highly likely that corporations will be unable to prevent or mitigate negative human rights impacts; an obligation imposed on companies by the United Nations Guiding Principles on Business and Human Rights. As such, continuing to conduct business in Russia entails significant legal risks for companies, including potential civil and criminal liability under comprehensive sanctions regimes and recent international jurisprudence holding corporations and their officers responsible for human rights abuses abroad.<sup>4</sup> By remaining in Russia, companies face the rising risk of criminal liability for complicity in international crimes, which can be prosecuted by domestic courts outside

---

<sup>2</sup> Federal Law No. 31-FZ of February 26, 1997 "On mobilization training and mobilization in the Russian Federation" (as amended), <https://base.garant.ru/136945/> (accessed November 14, 2022).

<sup>3</sup> Decree of the President of the Russian Federation No. 139 dated March 3, 2023 "On Certain Issues of Carrying Out the Activities of Business Companies Participating in the Fulfilment of the State Defense Order", <http://publication.pravo.gov.ru/Document/View/0001202303030004> (accessed March 22, 2023).

<sup>4</sup> International companies remaining in Russia are now at a greater risk of violating sanctions regimes as implementation of the legislation will likely involve transacting with sanctioned individuals or entities. Furthermore, new domestic civil and criminal cases against companies involved in violations of international law demonstrate the risk of significant liability for facilitating state-sponsored human rights abuses abroad (e.g., Lafarge case, Lundin case, Castel Group indictment, Nevsun holding, and Dassault Aviation, Thales, and MBDA France criminal complaint.) Victoria Riello and Larissa Furtwengler, "Corporate Criminal Liability for International Crimes: France and Sweden Are Poised To Take Historic Steps Forward," *Just Security*, September 6, 2021, <https://www.justsecurity.org/78097/corporate-criminal-liability-for-human-rights-violations-france-and-sweden-are-poised-to-take-historic-steps-forward/> (accessed November 14, 2022); The Sentry, "Breaking: France Opens War Crimes Inquiry Focused on Iconic Food and Beverage Conglomerate," July 1, 2022, <https://thesentry.org/2022/07/01/7216/breaking-france-opens-war-crimes-inquiry-focused-iconic-food-beverage-conglomerate/> (accessed November 14, 2022); Rfi, "French technology firm charged over Libya cyber-spying," July 2, 2022, <https://www.rfi.fr/en/business-and-tech/20210701-french-tech-firm-charged-over-libya-cyber-spying> (accessed November 14, 2022); Preston Lim, "Canadian Supreme Court Allows Corporate Liability for International Law Violations," *Lawfare*, March 12, 2022, <https://www.lawfareblog.com/canadian-supreme-court-allows-corporate-liability-international-law-violations> (accessed November 14, 2022); Sherpa, "Aiding and abetting war crimes in Yemen: Criminal complaint submitted against French arms companies," June 2, 2022, <https://www.asso-sherpa.org/aiding-and-abetting-war-crimes-in-yemen-criminal-complaint-submitted-against-french-arms-companies> (accessed November 14, 2022).

Russia under the doctrine of "universal jurisdiction."<sup>5</sup> Companies may also be exposed to financially material risks through operational restrictions, such as limitations of future government contracts.<sup>6</sup>

Firms which continue to trade with Russia also face high levels of risk attached to financial transactions. On 24 February 2023, the Financial Action Task Force (FATF) suspended Russia's membership as a result of the war, calling on all actors in the international financial system to exercise extreme caution in all dealings with Russia.<sup>7</sup> In practice, the decision means that all international banks will scrutinise all Russian payments, making financial transactions more expensive, lengthy, with no guarantee that the transaction will occur at all.<sup>8</sup> Although FATF has not yet blacklisted Russia, it highlighted the consensus among its 36 member countries that "the Russian federation's actions represent a gross violation of the commitment to international cooperation upon which FATF Members have agreed to implement and support the FATF Standards."<sup>9</sup> Previous practice shows that noncooperative behaviour is one of the reasons for FATF blacklisting. As a result, companies should examine and mitigate the high levels of risk attached to financial transactions with Russia and based on that risk, companies should reconsider all ongoing business operations related to Russia.

Additionally, the Ukrainian government's [National Agency on Corruption Prevention](#) (NACP) has created a list of "foreign companies that, despite the international recognition of Russia as the aggressor state and the introduced sanctions restrictions, continue to cooperate with it."<sup>10</sup> These companies are recognised as "international sponsors of war" by the Ukrainian state. The listed entities will be included into the World-Check database to protect the global financial sector from Russian sponsors of war. Since banks and insurance companies use World-check to assess risks, companies on the list will be limited in freely accessing personal and corporate finances. So far there are 21 companies on the list, but the NACP notes that it will be expanded with "international companies that provide the public and private sector with goods and services of critical purpose, as well as [those that] contribute to the Russian budget."<sup>11</sup>

---

<sup>5</sup> For example, ongoing proceedings in the US and France against the French multinational Lafarge for complicity in human rights violations in Syria. The Paris Court of Appeal, "La Cour d'appel de Paris confirme la mise en état de la multinationale française Lafarge pour complicité de crimes contre l'humanité commis par l'Etat islamique," May 18, 2022, <https://www.doughtystreet.co.uk/sites/default/files/media/document/Press%20release%20french%20version.pdf> (accessed March 22, 2023); United States Attorney's Office, Eastern District of New York, "Lafarge Pleads Guilty to Conspiring to Provide Material Support to Foreign Terrorist Organizations," October 18, 2022, <https://www.justice.gov/usao-edny/pr/lafarge-pleads-guilty-conspiring-provide-material-support-foreign-terroris> (accessed March 22, 2023).

<sup>6</sup> Venable LLP, "Do You Contract with State Governments? If So, Beware of Emerging State Sanctions' Obligations Related to Russia and Belarus," *JD Supra*, June 3, 2022, <https://www.jdsupra.com/legalnews/do-you-contract-with-state-governments-6537229/> (accessed January 2, 2022).

<sup>7</sup> FATF, "FATF Statement on the Russian Federation," February 24, 2023, <https://www.fatf-gafi.org/en/publications/Fatfgeneral/fatf-statement-russian-federation.html> (accessed March 14, 2023).

<sup>8</sup> Liudmyla Sliptsova, "Russia's membership in the FATF suspended. What does this mean and how ruinous is this for the aggressor's economy?," *Mind*, February 27, 2023, <https://mind.ua/en/publications/20253993-russias-membership-in-the-fatf-suspended-what-does-this-mean-and-how-ruinous-is-this-for-the-aggre> (accessed March 14, 2023).

<sup>9</sup> FATF (n 7).

<sup>10</sup> NACP, "International Sponsors of War," <https://sanctions.nazk.gov.ua/en/boycott/> (accessed February 6, 2023).

<sup>11</sup> NACP, "Companies from the NACP list of "International Sponsors of War" are now in the World-check database, used worldwide for reviewing counterparties," September 7, 2022, <https://nazk.gov.ua/en/news/companies-from-the-nacp-list-of-international-sponsors-of-war-are-now-in-the-world-check-database-used-worldwide-for-reviewing-counterparties/?hilit=sponsor+of+war> (accessed February 6, 2023).

In response to this unprovoked and unjustified war<sup>12</sup> many companies have already left Russia. According to the Kyiv School of Economics Institute's #LeaveRussia [company tracker](#), Microsoft has scaled back some of its operations, but is continuing others.

On March 4<sup>th</sup>, 2022, Microsoft announced that it suspended all new sales of Microsoft products and services in Russia, as well as stopped “many aspects of [its] business in Russia in compliance with governmental sanctions decisions.”<sup>13</sup> The statement also details Microsoft’s humanitarian aid to the people of Ukraine, as well as the actions the company has taken in order to provide improved cybersecurity to Ukraine, which is commendable.

In June, Microsoft announced further substantial cuts to its business in Russia, but that the company will fulfil its existing contractual obligations with its Russian customers.<sup>14</sup>

In September, Russian customers were reportedly unable to download the new Windows 10 and 11 OS updates. However, Russian media reports that as of December 2022 Microsoft has permitted Russians to download and install its Windows operating system and updates, including Windows 11, 10, Windows 8.1. and Windows 7.<sup>15</sup>

Last week, it was reported that Microsoft has been fined over \$3 million for supposedly breaching U.S. sanctions on Russia (and other countries). The reason behind the fine was that Microsoft’s software and services were found to have been acquired by blacklisted individuals and companies in the Crimea region of Ukraine. The breach led to the sale of \$12 million in products and services to blacklisted parties between December 2016 and December 2017.

The company allegedly uses an indirect resale model in Russia to develop sales leads and negotiate bulk sales with end customers, which ultimately resulted in the failure to obtain accurate information about some of these end users. Some of Microsoft’s Russian employees have reportedly intentionally circumvented the company’s screening procedures. The company’s spokesperson stated: “Microsoft takes export control and sanctions compliance very seriously, which is why after learning of the screening failures and infractions of a few employees, we voluntarily disclosed them to the appropriate authorities.”<sup>16</sup>

In light of Microsoft’s statements and the full-scale Russian invasion of Ukraine, we are writing now to enquire whether Microsoft has reconsidered its business practices that initially led to these sanction violations; what policies and practices has Microsoft employed to prevent such breaches from happening again; and what is the current exposure of Microsoft’s business in Russia.

These activities in Russia risk enabling and financing Russia’s violations of IHL and human rights law during the ongoing invasion and occupation of Ukraine.

---

<sup>12</sup> The UN General Assembly condemned Russia’s “aggression against Ukraine” and demanded that Moscow “unconditionally withdraw all of its military forces from the territory of Ukraine within its internationally recognized borders.”

<sup>13</sup> Microsoft, “Microsoft suspends new sales in Russia,” March 2, 2022, <https://blogs.microsoft.com/on-the-issues/2022/03/04/microsoft-suspends-russia-sales-ukraine-conflict/> (accessed April 11, 2023).

<sup>14</sup> Reuters, “Microsoft scales down Russia operations due to Ukraine crisis,” June 8, 2022, <https://www.reuters.com/technology/microsoft-cuts-russia-operations-due-ukraine-invasion-bloomberg-2022-06-08/> (accessed April 11, 2023).

<sup>15</sup> TASS, “Microsoft returned the ability to download and install Windows for Russians,” December 27, 2022, <https://tass.ru/ekonomika/16701537> (accessed April 11, 2023).

<sup>16</sup> Dylan Tokar, “Microsoft to Pay \$3 Million Over Russia Sanctions, Export Controls Violations,” *The Wall Street Journal*, April 6, 2023, <https://www.wsj.com/articles/microsoft-to-pay-3-million-over-russia-sanctions-export-controls-violations-14caa21> (accessed April 11, 2023).

We seek to understand the status of Microsoft's exposure to Russia and how Microsoft has conducted and continues to conduct heightened human rights due diligence, and how the findings of such a process have resulted in these continued business activities and relationships. As noted by the UNGPs:

...the more severe the abuse, the more quickly the enterprise will need to see change before it takes a decision on whether it should end the relationship. In any case, for as long as the abuse continues and the enterprise remains in the relationship, it should be able to demonstrate its own ongoing efforts to mitigate the impact and be prepared to accept any consequences – reputational, financial or legal – of the continuing connection.

In consideration of the above points and B4Ukraine's [Declaration](#), we request an urgent dialogue with Microsoft's relevant senior management and staff to discuss the company's ongoing activities and relationships in Russia, associated risks to the people of Ukraine and the company, and potential steps to prevent/mitigate these risks. Please contact the B4Ukraine Coalition at [contact@b4ukraine.org](mailto:contact@b4ukraine.org) to schedule a call. We kindly ask for your response by 5:00pm CET, April 25<sup>th</sup>, 2023.

Sincerely,

The B4Ukraine Coalition