Ethics Policy for Providers of Critical Digital Infrastructure

greenpeace.de

GREENPEACE

Table of Contents

Introduction

Big Tech as a Potential Enabler of Serious Environmental & Human Rights Violations

Big Tech corporations, in particular providers of critical cloud infrastructure such as **Amazon Web Services (AWS), Microsoft and Google**, are today the central »enablers« of the modern world. They provide the digital infrastructure — the foundation on which governments and economic actors operate, and within which interpersonal and societal interactions take place. This creates a position of power which carries risks that extend beyond purely technical matters:

- **Resource consumption:** The operation of cloud infrastructure consumes massive amounts of energy and raw materials, which increasingly conflicts with international environmental objectives such as the *Paris Climate Agreement* and the phase-out of fossil fuels.
- **Environmental and human rights violations:** At present, companies whose business models have destructive societal consequences (e.g., armaments, deforestation-driving or fossil-fuel enterprises) likewise benefit from the IT services provided.
- **Surveillance & military use:** Digital infrastructure may, for example, be deployed through the use of AI for the aggregation of large datasets or for the target acquisition of drones, and thereby misused to reinforce authoritarian structures or for military purposes in breach of international law.
- **Systemic dependency:** Acting as “bottlenecks”, cloud providers indirectly determine the market access of companies and the data sovereignty of entire economies and their citizens.

Big Tech companies, including cloud service providers, – like all companies – are not isolated economic actors but bear responsibility for their impacts on human rights, labour standards and the environment along the entire value chain. Economic history demonstrates that sectors characterised by a high degree of innovation dynamism and by systemically relevant business models in particular are subject to a heightened ethical duty towards society. The health and pharmaceutical sector, for example, places its business model in the service of the common good through centuries-old voluntary commitments and strict medicinal product authorisation procedures, thereby safeguarding it from abuse. The financial sector likewise defines ecological and social exclusion criteria for investments in the UN Principles for Responsible Investment (PRI). In the same manner, the tech sector must today live up to its role and responsibility as an innovator that promotes the common good, and must introduce ecological and ethical minimum standards that enable a good life for all.

The »Minimum Ethical Standard« for Cloud Providers

With the *Digital Services Act (DSA)*, the *Digital Markets Act (DMA)* and the *AI Act*, the EU has, in recent years, already established groundbreaking guardrails for the regulation of tech companies and AI development. Nonetheless, state regulation — particularly regional regulation — alone cannot keep pace with the speed of global technological disruption. Until state regulation catches up with technological progress, industry-wide voluntary commitments — of the kind known from the financial or pharmaceutical sector — are required in order to acknowledge the particular responsibility borne by digital »enablers«.

For providers of cloud infrastructure in particular, there exists a structural parallel with the financial sector: just as a bank enables certain projects by extending credit, a cloud provider enables countless new business models — such as *Software-as-a-Service (SaaS)*, *Infrastructure-as-a-Service (IaaS)* and *digital marketplaces — through computing power and IT services*, and increases the efficiency of existing business models. In the same way as financial institutions exclude the financing of controversial weapons, climate-damaging business models or rainforest deforestation, the present ethical minimum standards transfer these established principles to providers of cloud services. The policy defines the red lines which cloud infrastructure providers must draw in order to ensure that technological progress is not misused for pure profit maximisation and does not come at the expense of the common good.

The detailed policy set out below for providers of critical digital infrastructure is intended to translate these abstract ecological and ethical minimum standards into an operational reality that protects people and the environment and strengthens democratic structures. The policy serves as a template and is designed as a voluntary commitment ready for direct signature by companies. It demonstrates how global market leaders such as AWS, Microsoft and Google can embed their societal responsibility not merely in shiny sustainability reports, but in the form of effective rules of conduct that apply throughout their business model — from customer selection and the use of resources through to political influence. Such a commitment would be the requisite step towards evolving from a mere technology provider into a responsible actor shaping a democratic and sustainable digital future for all.

Ethics Policy

Preamble

As one of the world's leading providers of cloud infrastructure, we recognise that technology is not neutral and that its deployment is accompanied by societal responsibility. We hereby assume the responsibility associated with such deployment and, by means of the present policy, undertake to adopt binding measures which ensure that the services provided by us are not misused to harm the environment, to endanger human rights or to undermine democracies. The present policy shall ensure responsible economic conduct within planetary boundaries and shall apply to all business divisions, subsidiaries and partnerships.

1. USAGE RESTRICTIONS ON CLOUD SERVICES

We shall restrict the use of the infrastructure provided (computing power, storage, cloud services, etc.) and shall refrain from any joint product development in the following areas:

1.1 Fossil Fuels & Environmental Destruction

In accordance with international environmental instruments such as the *Paris Climate Agreement*, the *Convention on Biological Diversity (CBD)*, the *UN High Seas Treaty and* the *EU Deforestation Regulation (EUDR)*, the provision of infrastructure shall be excluded for the following companies and purposes:

- **Coal developers and coal-fired power generators:** Coal companies with expansion plans along the entire coal value chain (in accordance with Urgewald's Global Coal Exit List).
- **Expanding oil and gas companies:** Companies continuing to expand in fossil fuels (expansion in upstream and midstream operations), the construction of oil and gas pipelines for new fossil reserves, as well as new terminals for the export/import of LNG (in accordance with Urgewald's Global Oil and Gas Exit List).
- **Unconventional oil and gas extraction:** Companies engaged in fracking, tar sands, shale oil, and Arctic or deep-sea extraction (pursuant to the AMAP definition).
- **Companies with serious environmental controversies:** Companies causing serious, irreversible damage to ecosystems — for example, through deep-sea mining, through industrial activities such as the discharge of chemicals and waste, or through mining disasters (such as tailings-dam failures).
- **Deforestation companies:** Firms demonstrably involved in deforestation or unlawful land appropriation, unless they can demonstrate complete, verifiable traceability of their supply chain.
- **Concealment systems:** Systems designed to disguise the origin of agricultural commodities (»cattle laundering«) from protected areas (e.g. the Amazon, the Cerrado).

1.2 Human Rights Violations

In accordance with the *Universal Declaration of Human Rights*, the *UN Guiding Principles on Business and Human Rights* and the *UN Declaration on the Rights of Indigenous Peoples (UNDRIP)*, the provision of infrastructure shall be excluded for the following companies and purposes of use:

- **Serious human rights controversies:** The use of child labour and forced labour, precarious working conditions, the suppression of freedom of association, and systematic discrimination.
- **Violation of personal integrity:** In addition to physical and psychological violence, digital violence in the form of non-consensual pornographic content, and in particular deepfakes produced by means of generative AI.
- **Violation of indigenous rights:** Activities contributing to the unlawful appropriation of land, the destruction of cultural heritage, or the exploitation of resources in territories of indigenous peoples without their free, prior and informed consent (FPIC).

1.3 Weapon Systems & Military

In accordance with international conventions on prohibited weapon systems and the *EU AI Act*, the following military uses of cloud infrastructure shall be excluded:

- **Lethal Autonomous Weapon Systems (LAWS):** The development, manufacture and deployment of weapon systems that select and engage targets without meaningful human control (in accordance with the proposal of the NGO coalition »Campaign to Stop Killer Robots«).
- **Kinetic attack planning:** The direct target acquisition or operational execution of kinetic attacks.
- **Controversial weapon categories:** The development and use of cluster munitions, chemical and biological weapons, anti-personnel mines, blinding laser weapons, nuclear weapons, incendiary weapons containing white phosphorus, radiological weapons, depleted-uranium weapons, and non-detectable fragmentation munitions.

1.4 Surveillance, Repression & »Unacceptable Risks«

The use of cloud infrastructure (not only AI-related use) shall be prohibited for the following applications, which constitute an unacceptable risk pursuant to Article 5 of the *EU AI Act*:

- **Manipulative techniques:** The use of subliminal or deliberately manipulative techniques to influence a person's behaviour in such a manner as to cause significant harm to that person or to others.
- **Exploitation of vulnerabilities:** The targeted exploitation of a person's vulnerabilities by reason of age, disability, or a specific social or economic situation, in order to influence that person's behaviour in a harmful way.
- **Social Scoring:** The assessment of the trustworthiness of citizens giving rise to discriminatory consequences.
- **Predictive Policing:** The calculation of the probability of criminal offences on the basis of profiling or personality traits.
- **Biometric scraping:** The untargeted scraping of images of persons from the internet or from video surveillance in order to create or expand databases for facial recognition.
- **Emotion recognition:** The recognition of emotions in the workplace or in educational institutions.
- **Biometric categorisation:** The sorting of persons at national borders into specific categories (ethnicity, religion, sexual and political orientation) on the basis of biometric data.
- **Remote biometric identification:** Real-time facial recognition in public spaces by state or private actors.
- **Border surveillance:** The behavioural analysis of refugees or forecasting of migration movements that could give rise to pushbacks in breach of international law.

1.5 Disinformation & Democratic Integrity

The use of cloud infrastructure shall be prohibited for the following applications, which demonstrably undermine democratic structures:

- **Deepfakes & transparency:** The creation of manipulated content (audio/video) which, without appropriate labelling, is intended to influence elections or to deceive public opinion.
- **Anti-democratic groups:** Organisations seeking to undermine the free democratic order.

2. FAIR, ECOLOGICAL SUPPLY CHAINS & TRANSPARENCY

On the basis of the due diligence obligations set out in the *EU Corporate Sustainability Due Diligence Directive (CSDDD)*, we must deploy our market power in support of a fair, ecological supply chain and equitable infrastructure which places the protection of affected persons at its centre. We acknowledge that technological progress is inextricably linked to the livelihoods of local communities. From the electricity and water supply of data centres, through the mines used for raw-material extraction, to the digital labour of clickworkers, we bear the responsibility for ensuring that progress does not come at the expense of the most vulnerable participants in the supply chain.

2.1 Ecological Due Diligence & Transparency

- **24/7 Renewable Energy:** New computing capacity shall be operated exclusively with electricity from renewable energy sources (RES); certificates for green electricity are not sufficient. Renewables shall comprise wind, solar, geothermal and hydroelectric power. Nuclear energy shall not be included. Backup solutions shall likewise be based on RES.
- **Contribution to grid stabilisation:** Solutions such as demand-side management (flexible ramp-up/ramp-down) and battery storage shall be employed.
- **Closed cooling circuits:** Closed cooling circuits or dry cooling shall be used in all regions experiencing water stress. No drinking water shall be used for cooling purposes.
- **Waste-heat utilisation:** At least 25 percent of waste heat shall be re-used, with an 80 percent utilisation rate targeted in the longer term.
- **Disclosure obligation:** All relevant environmental indicators relating to energy and water consumption, as well as the electricity mix used, shall be reported both in aggregate and at the facility level.
- **Transparency regarding workloads:** We shall provide customers with verifiable, model-based estimates of the CO_2 and water footprint of each compute instance of a workload.

2.2 Clean & Fair Hardware Value Chain

- **Risk management & transparency:** Provision of a comprehensive risk map of the hardware supply chain (from mining to manufacture) which identifies ecological harm and quantifies the emissions of all IT components.
- **Active due diligence (leverage):** Compliance will be ensured by means of binding contractual clauses and technical support obliging suppliers to adhere to EU environmental and human rights standards.
- **Remedy & stakeholder involvement:** Implementation of transparent remediation processes in the event of breaches of the policy, guaranteeing the protection of environmental defenders and compensation for affected communities (for example, for loss of land, health impacts), with the direct involvement of local actors.
- **Circularity & e-waste:** Demonstrable evidence, by 2030, that hardware, following replacement, shall primarily be re-used in »second-life« programmes or materially recycled to at least 90 percent.
- **Accountability:** Publication of an annual due diligence statement which auditably documents progress in risk prevention, Scope 3 reduction and recycling rates.

2.3 Labour Protection for Clickworkers

- **Transparency of the digital supply chain:** Transparency regarding the geographical distribution and labour standards of clickwork. No services shall be used where there are indications of child labour, forced labour or modern slavery (in accordance with the *ILO Core Labour Standards* and the *UK Modern Slavery Act*). This shall apply in particular to the assignment of microtasks in high-risk regions where the platform does not demonstrate adequate control mechanisms.
- **Compliance with ILO principles and national labour laws:** The above shall apply to all clickworkers performing work for or on behalf of our services. This shall include fair remuneration aligned with local living-wage standards, freedom of association and the right of workers to organise in trade unions, and independent auditing of working conditions on the platform.

3. POLITICAL INTEGRITY & TRANSPARENCY ON LOBBYING

- **No erosion of existing climate-protection and tech regulation:** We shall refrain from actively opposing climate, environmental and tech regulation, including the *EU Energy Efficiency Directive (EED)*, the *Digital Markets Act (DMA)* and the *Digital Services Act (DSA)*.
- **Transparency regarding network and lobbying expenditure:** Annual publication of all lobbying expenditure, broken down by in-house personnel, lobbying agencies, industry associations, think tanks, image campaigns and other local initiatives such as events and sponsorships.
- **Transparency regarding personal meetings:** Publication of the minutes of all high-level meetings with EU Commissioners and Members of Parliament. Furthermore, going beyond the statutory obligation, the disclosure of all meetings with political actors in the lobby register.

4. COMPLIANCE & ENFORCEMENT OF THE POLICY

A policy without monitoring processes is ineffective. Efficient control mechanisms shall therefore be established.

- **Embedding a process for implementation and monitoring of the ethics policy:** No business relationships shall be entered into with customers whose activities breach the rules set out in Chapter 1. Engineers shall be granted the contractually secured right to refuse to work on projects that infringe this policy, without suffering professional disadvantage.
- **Fundamental rights impact assessment:** We undertake to require, from all customers operating high-risk systems within the meaning of the *EU AI Act*, evidence of a completed fundamental rights impact assessment, irrespective of whether such customers are public or private entities.
- **Independent Ethics Council:** An independent, external ethics council comprising representatives from civil society and academia shall be convened. The council shall publish official recommendations concerning the termination of cooperation with critical customers.

NO MONEY FROM INDUSTRY OR GOVERNMENT

Greenpeace is an independent campaigning network which uses non-violent, creative confrontation to expose global environmental problems and to force solutions which are essential for a green and peaceful future.

Fight the billionaire takeover and corporate intimidation

Billionaires and corporations are tightening their grip on our democracies — and silencing dissent. They weaken protections for people and the planet, bankroll politicians who serve their interests, control media narratives, and use corporate intimidation to shut down free speech.

Time to resist!

Sign the petition:
greenpeace.org/international/act/time-to-resist/

Imprint

Greenpeace e.V. Hongkongstraße 10, 20457 Hamburg, Germany T +49 (0)40 30618-0, mail@greenpeace.de, greenpeace.de, **Political Unit Berlin** Marienstraße 19–20, 10117 Berlin, Germany T +49 (0)30 308899-0 **Legally responsible for content** Marie Kuhn **Text** Marie Kuhn **Coverpage** tuckow.studio **Photos** © istockphoto [M] **Layout** Andrea Bayer **Published** 05 / 2026